

# CONNECTÉ ET ÉCLAIRÉ

## SE PROTÉGER EN LIGNE



World Association  
of Girl Guides  
and Girl Scouts

Association mondiale  
des Guides et des  
Eclaireuses

Asociación  
Mundial de las  
Guías Scouts





## SOMMAIRE

Introduction .....	01
Comment utiliser ce kit d'animation .....	02
Conseils pour les éducateurs .....	02
Lignes directrices de sécurité Internet pour les adultes .....	03
Jeux de mise en condition .....	06
Activités « connecté et éclairé » .....	09
<b>Se connecter</b> - positivement en ligne .....	09
<b>Se protéger</b> - soi-même des risques en ligne .....	17
<b>Se respecter</b> - vos droits, vos valeurs et votre réputation en ligne .....	23
Choisissez votre propre sécurité d'abord ! .....	31
Ressources et liens .....	33
Glossaire .....	34



## INTRODUCTION

### POUVEZ-VOUS IMAGINER LA VIE SANS INTERNET ?



En une vingtaine d'années seulement, nous avons intégré le réseau mondial dans nos vies, dans un si grand nombre de domaines, qu'il est difficile de croire que nous ayons pu vivre sans ! D'ici 2015, on prévoit qu'il y aura 15 milliards d'appareils (ordinateurs, smartphones...) reliés à

internet dans le monde. Ce qui correspond à deux appareils par personne sur la planète ! Beaucoup d'entre nous ne peuvent imaginer un monde où internet ne serait pas accessible du bout des doigts. Un grand nombre de personnes nées dans les vingt dernières années ont déjà oublié l'époque où internet ne faisait pas partie de leur vie. Chaque jour, un nombre croissant d'individus a accès à internet.

Les idées nouvelles et les évolutions technologiques rendent nos vies en ligne à la fois plus riches et plus complexes. Bien que 60% de la population mondiale soit privée d'accès à internet, ce pourcentage diminue de jour en jour. Étant donné que le monde en ligne s'ouvre de plus en plus aux jeunes, il est primordial que nous fournissions à nos membres des outils pour leur permettre d'avoir confiance et de se protéger sur internet.

L'Association mondiale des Guides et des Éclaireuses (AMGE) fait le constat qu'internet occupe une large place dans la vie de ses membres. Ceux qui ont un accès au web y passent en moyenne plus d'1h30 chaque jour, quel que soit le lieu où ils vivent dans le monde. Lorsqu'ils sont "connectés", ils peuvent interagir avec d'autres personnes à travers le globe, s'exprimer sous des formes nouvelles, mettre en place de nouveaux modes de communication, déployer des compétences sociales et avoir accès à des informations qui leur permettent de faire des choix de vie mieux éclairés. Il nous faut changer notre façon de percevoir les jeunes en ligne. Nous ne pouvons pas protéger nos membres en restreignant leur accès à internet. Quand ils grandissent, ils ont besoin de profiter des avantages qu'offre internet et ils ont le droit de le faire en sécurité et d'être bien informés sur la manière de se protéger eux-mêmes en ligne.

La manière dont nous interagissons sur internet change à la vitesse de la lumière et les espaces en ligne ne sont plus seulement des sources d'information. Il s'agit de communautés qui attendent des utilisateurs qu'ils apportent des contributions en publiant, chargeant, commentant, partageant et créant des tags. Avec la croissance rapide de

l'internet mobile, ces interactions deviennent une extension de nos vies quotidiennes. Les enfants vivent perpétuellement sur cette vague, adoptant souvent les nouveaux outils en ligne, avant même que leurs parents en aient entendu parler. L'âge auquel les enfants ont accès à internet pour la première fois est de plus en plus précoce. Selon le rapport 2011 d'EU Kids Online (Enfants européens en ligne), l'âge moyen de la première utilisation d'internet en Europe est de neuf ans, et l'utilisation des réseaux sociaux suit peu de temps après. Bien qu'un grand nombre de réseaux sociaux n'autorisent l'accès aux enfants qu'à partir de 13 ans, 38% des 9-12 ans ont créé des profils sur les réseaux sociaux en falsifiant leur âge lors de leur inscription.

Plus les enfants se connectent, plus ils s'exposent aux risques d'internet. Dans son rapport 2010 sur la Famille en ligne, Norton a découvert que presque les deux tiers des enfants avaient fait une mauvaise expérience en ligne, mais que seulement 45% des parents en avaient pris conscience. Les enfants se responsabilisent de plus en plus vis-à-vis des expériences négatives en ligne. Un tiers d'entre eux ressentent ces expériences négatives comme risquant de porter atteinte à leur bien-être émotionnel.

En tant qu'organisation mondiale, l'AMGE a expérimenté l'impact positif de l'introduction des nouvelles technologies dans son travail. Internet rapproche nos membres présents dans 145 pays et leur permet de prendre la parole comme une seule voix sur des problématiques qui affectent leurs vies. Il peut également offrir des manières innovantes de mettre en place des connexions locales, donnant plus d'autonomie aux groupes de guides et d'éclaireuses avec de nouveaux outils pour apporter du changement dans leurs communautés. Au moment où l'AMGE est aussi en cours de processus d'exploration des possibilités de l'apprentissage à distance pour enrichir nos programmes de leadership et de formation, il est essentiel que nous procurions à nos membres les outils nécessaires pour s'engager en sécurité dans de prochaines initiatives d'apprentissage en ligne.

Nous adressons nos remerciements tout particulièrement à Symantec qui apporte son soutien à cette initiative. Sans son appui, ce kit d'animation n'aurait pu être réalisé. Nous espérons que ces activités fourniront à nos membres l'autonomie nécessaire pour utiliser internet de manière sûre et confiante. Le but étant de leur permettre de profiter des opportunités offertes en ligne, afin de développer pleinement leur potentiel de citoyens du monde, conscients de leurs responsabilités.

**Nadine El Achy**

Présidente du Conseil mondial.



## INTRODUCTION

### COMMENT UTILISER CE KIT D'ANIMATION ?

Un peu plus de 30% de la population mondiale a accès à internet. Si vous faites partie des personnes "connectées", internet joue probablement un grand rôle dans votre vie. Vous l'utilisez pour répondre à vos questions, échanger avec vos amis et profiter de votre temps libre. Le but de ce kit est de vous aider à mieux tirer parti du temps que vous passez en ligne, découvrir comment vous pouvez utiliser internet pour mettre au jour des opportunités intéressantes, vous relier à des communautés locales ou mondiales et partager certains conseils sur la manière de vous protéger lorsque vous êtes connectés sur le web.

Ce kit commence avec des jeux de mise en condition : une façon de vous offrir une introduction ludique aux idées qu'il explore. Ensuite, vous trouverez une liste d'activités que vous pouvez utiliser avec les jeunes.

Les activités ont été regroupées en trois thèmes :

**Se connecter...** positivement en ligne

**Se protéger...** soi-même des risques en ligne

**Se respecter...** vos droits et votre réputation en ligne

Pour devenir un véritable surfeur averti, vous devez accomplir six activités, deux pour chacun des thèmes, plus l'activité « Choisissez votre propre sécurité d'abord ! »

Tout au long de ce kit, vous trouverez des encadrés avec des informations générales sur des sujets spécifiques, des faits intéressants et des conseils pratiques pour vous aider à tirer le meilleur parti du temps que vous passez en ligne. En parcourant le kit, il se peut que vous rencontriez des mots qui sont nouveaux pour vous. Ceux-ci sont expliqués dans le glossaire en page 34.

<13 ANS      13 ANS +      TOUS ÂGÉS



DISCUSSION



PROLONGEZ  
L'EXERCICE



### CONSEILS POUR LES ÉDUCATEURS

La sécurité sur internet est une question importante à se poser, l'accès à internet se répand toujours davantage, et les jeunes ont plus d'occasions de l'intégrer dans leur vie quotidienne. L'objectif de ce kit est de sensibiliser à la question de la sécurité sur internet le plus grand nombre possible de membres dans les groupes de scouts et guides et d'éclaireurs et éclaireuses. Par conséquent, nous vous encourageons à adapter les activités afin de les rendre aussi accessibles que possible à tous vos membres. C'est vous qui les connaissez le mieux !

Les activités de ce kit ont été élaborées pour les membres de l'AMGE de tout âge, des deux sexes et avec l'apport de divers pays. Certaines activités ont été identifiées comme étant plus adaptées à des membres plus âgés ou plus jeunes, mais fiez-vous à votre propre jugement dans le choix des activités pour votre groupe. S'il est important que nos membres soient sensibilisés à la manière de se protéger en ligne dans toutes les situations, ce kit vise avant tout à encourager, et non à pousser nos membres à se connecter.

Nous recommandons que les activités qui nécessitent de passer du temps en ligne soient réservées aux membres de 13 ans et plus. Ceci, parce que certains services en ligne utilisés couramment, comme Facebook et YouTube, ne sont pas destinés à des enfants de moins de 13 ans. Cependant, il ne s'agit que d'une ligne directrice et vous pouvez considérer que beaucoup de ces activités conviennent à des membres plus jeunes. Étant donné que les enfants apprennent maintenant à se servir d'internet dès qu'ils sont scolarisés, si ce n'est plus tôt, nous pensons qu'il est important que nos membres commencent à aborder la sécurité sur internet le plus rapidement possible.

Prenez connaissance des informations contenues dans ce kit avant de commencer le programme. Notez également que, tandis que les liens en ligne que nous avons choisis nous paraissent appropriés à une audience de jeunes, nous vous conseillons de les vérifier au préalable pour avoir l'assurance qu'ils conviennent bien à votre groupe. Il est de votre responsabilité de vous assurer que tous les garde-fous ont été mis en place, et que vous avez obtenu les consentements nécessaires lorsque vous utilisez cette ressource. Pour ce faire, veuillez faire usage des lignes directrices de sécurité sur internet ci-après, destinées aux adultes.

Enfin, nous vous encourageons à ajouter tout contenu pertinent que vous êtes susceptible de découvrir au cours de vos propres recherches. Vous trouverez des vidéos, de la musique, des photos, des jeux et quantité d'informations sur YouTube et les sites internet répertoriés au dos de ce kit.

## LIGNES DIRECTRICES DE SÉCURITÉ INTERNET POUR LES ADULTES

Ces lignes directrices s'adressent aux parents et éducateurs des scouts, guides, éclaireurs et éclaireuses. Elles ont pour but de vous aider à comprendre comment protéger au mieux les jeunes dont vous êtes responsables, en ce qui concerne leur sécurité et leur vie privée. Certains points sont des exigences légales dans certains pays, mais pas dans d'autres. Par conséquent, ils peuvent être considérés comme de bonnes pratiques, même s'ils ne sont pas juridiquement contraignants.

Considérez la manière dont vous protégez les enfants dans la vie réelle. Vous veillez à les tenir à l'écart de situations dangereuses physiquement. Vous surveillez le lieu où ils se trouvent, avec qui ils sont, ce qu'ils regardent et comment ils se comportent. Maintenant, appliquez ces mêmes critères à leurs interactions internet et numériques et pensez aux manières de réduire les menaces potentielles et de vous assurer que les enfants soient protégés et en sécurité. En tant qu'éducateur, vous devez prendre soin de maîtriser vos activités en ligne, et de distinguer votre vie privée et publique.



### Politique des emails

- Créez un système d'emails pour votre groupe. Choisissez un volontaire adulte pour se charger de l'ajout, de la modification et de la suppression d'adresses email du système. Établissez des listes de diffusion pour les parents/responsables, les membres de chaque tranche d'âge et les éducateurs de groupe.
- Utilisez la fonction "copie carbone invisible" (cci) lorsque vous adressez des mails à des groupes pour protéger les coordonnées de chacun(e) et éviter les spams.
- N'utilisez la liste qu'à des fins de communication au sein du groupe de scouts et guides, d'éclaireurs et éclaireuses. Ne transmettez pas des emails en chaîne à des jeunes. Ne partagez pas la liste avec des personnes non membres.
- Évitez les communications privées directes avec les enfants, autres que les messages généraux adressés au groupe.
- Si vous voulez prendre contact avec un jeune de moins de 16 ans par email ou par courrier, vous devez obtenir une permission écrite de ses parents/responsables. Dans tout message que vous adressez à un jeune de moins de 18 ans, ajoutez le nom d'un autre adulte en copie.
- Si un enfant prend directement contact avec vous ou un autre éducateur adulte, discutez-en avec d'autres adultes pour savoir comment agir au mieux pour traiter cette question. En fonction de la nature de la communication, réfléchissez s'il est nécessaire d'avertir les parents/responsables de l'enfant. Votre réponse pourra varier en fonction de l'âge de l'enfant : un membre plus âgé du groupe de scouts et guides ou d'éclaireurs et éclaireuses peut interagir avec les éducateurs bien que les parents/responsables doivent en être informés lorsque l'enfant rejoint le groupe.
- Réfléchissez au contenu de votre message, en contrôlant que le vocabulaire et les images sont appropriés à la tranche d'âge et vérifiez où conduisent les liens.





## LIGNES DIRECTRICES DE SÉCURITÉ INTERNET POUR LES ADULTES

### Politique de réseau social

- Si créer un réseau social doit profiter à votre groupe, assurez-vous que le groupe que vous créez est privé.
- Invitez les membres du groupe d'un âge approprié, ainsi que leurs parents, à rejoindre la page ou le site du réseau social du groupe. Ayez à l'esprit que les réseaux sociaux sont soumis à des politiques différentes en fonction de l'âge. Par exemple, les membres de moins de 13 ans ne doivent pas avoir un compte Facebook ou utiliser YouTube. Utilisez des paramètres de confidentialité stricts pour empêcher que les posts et les photos soient vus par des personnes non membres de votre groupe. Lorsqu'un membre part, assignez à un volontaire adulte la responsabilité de supprimer du groupe les coordonnées du membre et de ses parents/responsables.
- Créez une politique pour déterminer si les adultes et les jeunes membres peuvent ou ne peuvent pas s'accepter mutuellement comme amis sur les réseaux sociaux. Recueillez le consentement parental avant d'accepter l'"amitié" en ligne d'un enfant.
- Définissez votre responsabilité et les mesures qui s'imposeraient, si vous observiez qu'un jeune publie des posts avec un langage, des images et des liens inappropriés.
- Évitez les communications privées directes avec des enfants, autres que les messages généraux qui s'adressent au groupe. Si un enfant s'adresse directement à vous ou à un autre éducateur adulte, discutez avec d'autres volontaires adultes de la manière de traiter cette question (voir la politique des mails ci-dessus).



### Politique photos et vidéos

- Créez une politique pour votre groupe pour déterminer si vous prendrez des photos ou pas des activités de groupe, et obtenir le consentement signé des parents/responsables sur cette politique avant de prendre des photos de leurs enfants. Précisez si les photos seront partagées avec les membres du groupe et leurs parents ou pas. Tandis que la plupart des parents apprécieront de conserver ces photos et vidéos en souvenirs, certains peuvent refuser que des photos de leur enfant soient prises et/ou partagées pour des raisons d'ordre religieux, privé ou autre. Si des parents refusent le partage de photos, ayez à l'esprit lorsque vous réalisez des photos et des vidéos, que leurs enfants ne doivent pas figurer dessus.
- Si vous mettez en place des pages en ligne de partage de photos et de vidéos, elles doivent être privées et protégées de préférence avec un mot de passe. Obtenez le consentement de toute personne figurant sur les photos/vidéos avant de les charger.
- Prenez un instant pour réfléchir avant de partager des photos et des vidéos de jeunes en ligne et de faire des marquages de noms dans les images (tags). Si vous voulez partager un contenu, vérifiez que vous avez obtenu la permission par écrit des parents/responsables avant d'y procéder.

## LIGNES DIRECTRICES DE SÉCURITÉ INTERNET POUR LES ADULTES



### Sécurité en ligne en général

- Sécurisez votre propre ordinateur et autres périphériques : Assurez-vous que votre ordinateur personnel et les autres périphériques connectés à internet sont protégés des virus et logiciels malveillants par l'utilisation de logiciels de sécurité sur internet. Soyez vigilant(e) par rapport à la détection de logiciels malveillants. De cette façon, vous pourrez empêcher la propagation à d'autres membres du groupe ou l'accès non autorisé aux données privées des membres et informations financières mémorisées sur votre ordinateur ou autre périphérique.
- Utilisez des mots de passe pour protéger vos périphériques : Les enfants peuvent demander d'emprunter ou d'utiliser le téléphone, la caméra numérique, la tablette ou l'ordinateur d'un adulte volontaire. Vous pouvez les empêcher d'accéder à des fichiers ou des programmes spécifiques sur ces appareils en utilisant des mots de passe lorsque cela est possible. Assurez-vous qu'il n'y ait pas de contenu répréhensible mémorisé sur votre appareil. Si tel est le cas, vous pouvez être sûr qu'un enfant le trouvera. Un mot de passe peut également empêcher un enfant d'acheter de la musique ou des applications sans votre permission.
- Services bancaires en ligne : Il faut demander à la trésorière de votre groupe de sécuriser son ordinateur avec un logiciel de sécurité sur internet et de surveiller attentivement qui peut avoir accès au compte bancaire du groupe, que ce soit physiquement ou en ligne. Évitez de procéder à des transactions financières pour le groupe sur des ordinateurs publics ou sur des réseaux publics

sans fil qui sont susceptibles d'avoir moins de paramètres de sécurité que votre réseau personnel. Contrôlez le compte en ligne au moins une fois par semaine et vérifiez que les transactions sont toutes autorisées. En cas d'activité suspecte, faites en état à votre banque immédiatement pour minimiser les pertes sur le compte.

- Mémorisation des inscriptions des membres : Qui conserve les formulaires d'inscriptions des membres de votre groupe ? Ces informations qui comportent des noms, des numéros de téléphone, des adresses email et de domicile, des données relatives à l'assurance maladie et des liens vers des bases de données peuvent intéresser un voleur d'identité. Fixez des règles pour le stockage et la protection des copies physiques et numérisées de ces formulaires.

### Protection des membres du groupe

- Si un jeune vous confie qu'il a le projet de rencontrer quelqu'un avec qui il a fait connaissance sur internet, assurez-vous que ses parents en soient informés. Si les parents/responsables autorisent la rencontre, recommandez qu'ils accompagnent l'enfant et s'assurent qu'elle se tient dans un lieu public. Tandis qu'un grand nombre de personnes nouent de nouvelles relations amicales authentiques en ligne, les inquiétudes sont justifiées lorsqu'il s'agit de rencontrer quelqu'un, sans être à même au préalable, d'établir si cette personne est bien celle qu'elle prétend être.
- Si vous découvrez que des enfants sous votre supervision sont engagés dans des activités en ligne potentiellement dangereuses, comme visiter des sites pour adultes ou d'autres sites inappropriés, utiliser des dispositifs de partage illicite de fichiers ou rejoindre des groupes de réseaux sociaux qui encouragent des comportements antisociaux, vous devez définir vos responsabilités vis-à-vis des enfants, de leurs parents/responsables et de la communauté et agir en conséquence. Discutez de la meilleure approche avec les autres éducateurs adultes. N'ayez pas peur de "tirer la sonnette d'alarme" et d'alerter les parents/responsables sur les risques et dangers potentiels.



## JEUX DE MISE EN CONDITION

Ces activités facultatives peuvent être utilisées également comme activités rapides pour commencer une réunion ou remplir une courte fenêtre temporelle. Lorsque vous travaillez avec des enfants ou des jeunes en situation de handicap, vous pouvez décider de ne réaliser qu'une sélection de ces activités.

### 1. Quel est le message ?

Remettez à chacun un morceau de papier et asseyez-vous en cercle. La première personne murmure un mot à son voisin, qui dessine ce qu'il a entendu sur le papier et le passe à la troisième personne, qui murmure ce qu'elle voit à la personne suivante et ainsi de suite avec le message alternant entre mots et dessins. Le message est-il le même lorsqu'il revient au début ? Commencez avec des objets ou des expressions simples, puis rendez le message plus complexe. Demandez à votre éducateur de choisir secrètement une personne dans le cercle qui changera un mot du message. Pouvez-vous déterminer où il a été modifié ?

Comment les messages peuvent-ils être modifiés en ligne ? Lorsque vous avez publié des informations en ligne, quel niveau de contrôle avez-vous sur celles-ci ?

### 2. C'est ce que vous savez

Chacun écrit sur des bandes de papier deux ou trois faits sur un personnage imaginaire et les place dans un récipient. Partagez le groupe en deux équipes et placez le récipient rempli à un point de départ et un récipient vide à un point d'arrivée. Ils doivent être aussi éloignés l'un de l'autre que possible dans un grand espace intérieur ou extérieur. L'équipe

A se rassemble au point de départ et l'équipe B se répartit dans l'espace. À l'annonce de "Partez", chaque membre de l'équipe A prend une bande de papier et essaie de la placer dans le récipient vide sans se faire attraper. Si les membres de l'équipe A se font attraper, l'équipe B prend la bande de papier. Le jeu continue avec tous les joueurs jusqu'à ce que toutes les bandes de papier soient ou bien dans le récipient d'arrivée ou bien capturées par l'équipe B. Lorsque le jeu est terminé, chacun écoute ce que l'équipe B a appris au sujet du personnage imaginaire.

Que se passerait-il si le personnage imaginaire, c'était vous, et que ces faits étaient des informations que tout le monde pourrait voir sur internet ? Comment vous sentiriez-vous ? Que pensez-vous qu'un cybercriminel pourrait faire avec ces informations ?

### 3. Des vers et des murs

Un membre du groupe est désigné pour être l'utilisateur de l'ordinateur. Six autres se tiennent par la main et forment un cercle autour de lui/d'elle. Ils représentent le logiciel de sécurité qui protège l'ordinateur. Quatre membres deviennent des logiciels malveillants essayant d'avoir accès à l'ordinateur. Lorsque le leader dit "Partez", les logiciels malveillants essaient de toucher l'utilisateur de l'ordinateur, tandis que le logiciel de sécurité essaie de les éloigner. Ensuite, retirez trois ou quatre membres qui constituent le logiciel de sécurité, et dites au groupe que l'utilisateur de l'ordinateur n'a pas mis à jour son logiciel. Recommencez le jeu. Est-ce plus facile pour le logiciel malveillant d'atteindre l'utilisateur de l'ordinateur ?

Pourquoi est-ce important d'utiliser un logiciel de sécurité et de le mettre à jour ? Que pouvez-vous faire d'autre pour protéger votre ordinateur et les informations mémorisées ?



## JEUX DE MISE EN CONDITION



### 4. Piratage de mots de passe

Un bon mot de passe utilise un mélange de lettres, de chiffres et de symboles. Il doit être difficile à deviner par autrui, mais facile à mémoriser pour vous. En petit groupe, chacun à son tour choisit un objet mémorable ou une expression ou un dicton favori, comme une ligne extraite de votre livre ou film préféré. Chaque personne réfléchit alors à la manière de transformer cette expression en mot de passe difficile à deviner mais facile à mémoriser avec au moins huit caractères, en utilisant un mélange de lettres, de chiffres et de symboles. Pour vous aider, représentez un tableau avec deux lignes et autant de colonnes qu'il y a de lettres différentes dans votre mot de passe. Si vous utilisez une expression, utilisez la première lettre de chaque mot. Écrivez les lettres dans la ligne supérieure et un symbole ou un chiffre correspondant en dessous. Par exemple, voici comment le mot facile à deviner "butterfly" devient "B@++3rf1Y", qui est un bien meilleur mot de passe.

B	U	T	E	R	F	L	Y
B	@	+	3	R	F	1	Y

Écrivez quelques mots de passe en utilisant ce code, puis donnez vos mots de passe à un(e) ami(e) et voyez s'il (si

elle) peut les déchiffrer.

Pouvez-vous réfléchir à d'autres manières de composer un mot de passe compliqué mais facile à mémoriser ?

### 5. Bloquez-le !

Organisez une course d'obstacles sur votre lieu de réunion. Bandez les yeux de deux membres de votre équipe et demandez-leur de marcher d'une extrémité à l'autre du parcours. Chacun a un "guide" qui marche avec lui mais le guide ne peut aider que par la voix. Quel est le niveau de difficulté pour effectuer le parcours sans toucher les obstacles ?

Ce jeu reproduit un peu ce qui se passe en ligne. La personne qui a les yeux bandés est comme celle qui utilise internet et ne peut pas toujours voir les risques en matière de sécurité qui l'environnent. Le guide représente le logiciel de sécurité qui peut aider l'utilisateur à naviguer sur le web en sécurité. Cependant, les logiciels de sécurité ne peuvent pas tout par eux-mêmes. La personne qui a les yeux bandés doit coopérer et être prudente, en faisant appel à ses autres sens et en ne fonçant pas bille en tête. Les utilisateurs d'internet doivent être aussi avisés et prudents que possible. Cette attitude, combinée à la mise en place d'un bon logiciel de sécurité, doit contribuer à leur sécurité en ligne.



## JEUX DE MISE EN CONDITION

### Quel est le modèle ?

Un volontaire quitte la pièce et le reste du groupe s'assoit en cercle et choisit une personne pour démarrer une action comme frapper des mains, tapoter sur sa tête ou sur ses genoux. Cette personne peut changer d'action à tout moment et les autres doivent suivre. Le volontaire est rappelé, se tient au milieu du cercle et essaie de désigner la personne qui change l'action. Il a deux chances pour le deviner. Rejouez plusieurs fois.

Quel est le niveau de difficulté pour désigner la personne responsable du changement d'action ? Quel serait ce niveau de difficulté s'il fallait repérer la personne responsable du lancement d'une rumeur ou de l'envoi d'un message en ligne ? Serait-il plus facile d'identifier d'où vient le message si tout le monde ne copiait pas la personne changeant d'action ou répandant un message ?

### Arrêtez ce post !

Placez une personne à chaque extrémité de l'espace de réunion. L'une est l'émetteur et l'autre le récepteur. Remettez un petit objet, comme une balle de ping-pong à l'émetteur. Elle représente un message publié en ligne. Le reste du groupe se partage en deux équipes. Une équipe essaie de faire passer le post d'une extrémité à l'autre de la salle en le faisant transiter secrètement par le plus grand nombre possible de membres. L'autre équipe essaie d'identifier qui détient le post et l'arrête en touchant au bras la personne qui détient l'objet. Encouragez différentes stratégies comme la vitesse et l'esquive, l'action subtile et secrète, ou la distraction de l'équipe qui cherche.

Les messages peuvent se répandre très rapidement en ligne. Que pensez-vous pouvoir faire pour vous assurer que les posts en ligne n'auront pas de conséquences négatives ?

### 6. Détectez la différence !

Un volontaire quitte la pièce. Le reste du groupe choisit un scénario et quelque chose qui rend le volontaire différent. Par exemple, les membres du groupe sont des plongeurs sous-marins et le volontaire est une sirène. Le groupe commence à improviser le scénario. Le volontaire revient, se joint à l'improvisation et essaie de deviner ce qu'incarnent les membres du groupe et ce qu'il est lui-même dans sa différence. Le volontaire peut échanger avec le groupe et poser des questions. Répétez le jeu plusieurs fois avec différents volontaires et scénarios.

Qu'avez-vous ressenti en étant différent ? Est-ce que le groupe était accueillant ou antipathique ? Aurait-il pu se comporter différemment ? Dans quelle mesure cette expérience vous renvoie-t-elle à vos expériences en ligne ?

### 7. Court ou long ?

Remettez à chacun trois objets à inclure dans un récit. La moitié du groupe doit inventer un récit de la longueur qu'il souhaite. L'autre moitié ne peut utiliser que 140 caractères pour rédiger son récit. Faites partager les récits. Quel groupe a trouvé que c'était plus facile de raconter une bonne histoire ?

Des posts courts sur les réseaux sociaux peuvent rendre vos messages difficiles à faire passer. Quels sont, selon vous, les types de messages qui fonctionnent bien sur les réseaux sociaux ? Y a-t-il d'autres messages qu'il est préférable de faire partager par des méthodes différentes ?

### 8. Franchir la ligne

Rassemblez le groupe dans le milieu de la salle et expliquez qu'on attribue les mots "vrai" ou "accord" à une extrémité de celle-ci et "faux" ou "désaccord" à l'autre extrémité. Lisez les informations et les conseils que l'on trouve dans ce kit, tels que "vous ne devez jamais utiliser votre vrai nom dans un forum". Les membres courent vers l'extrémité de la salle qui illustre leur réponse.



## ACTIVITÉS CONNECTÉ ET ÉCLAIRÉ

## SE CONNECTER POSITIVEMENT EN LIGNE

Choisissez deux activités dans chaque thème ci-dessous, plus l'activité "Choisissez votre propre sécurité d'abord !" page 33.

1

### CE QUE CELA SIGNIFIE POUR MOI

Internet a pris une large part dans nos vies très rapidement. Dressez une liste des différentes manières dont, selon vous, internet touche votre vie. Prenez en compte les aspects positifs et négatifs. Demandez aux personnes que vous connaissez qui appartiennent à une génération différente, comme les parents et les grands parents, comment ils utilisent internet dans leur vie quotidienne et dans quelle mesure la vie d'aujourd'hui est différente de celle qu'ils ont connue dans leur jeunesse. Dans quelle mesure leurs réponses diffèrent-elles et pourquoi, selon vous, est-ce le cas ? Ensuite, imaginez que vous vous interviewiez vous-même avec vingt ans de plus. Comment, à votre avis, l'impact de la technologie sur votre vie aura changé ? Créez une présentation des réponses sous forme d'affiches, prospectus, posts ou vidéo sur un blog.



**Prolongez l'exercice** – Choisissez une personne d'une précédente génération dont vous pensez qu'elle a changé le monde, comme Emmeline Pankhurst, Mahatma Ghandi, Rosa Parks ou Nelson Mandela. Pensez-vous qu'ils auraient agi différemment s'ils avaient disposé d'un compte sur un réseau social ?

2

### CONNECTEZ-VOUS

Internet n'est pas la seule manière de se connecter. En tant que scouts/guides ou éclaireurs/éclaireuses, vous faites partie d'un Mouvement mondial qui rapproche des jeunes de 145 pays. Recherchez différentes méthodes pour entrer en contact avec un groupe de scouts/guides ou d'éclaireurs/éclaireuses, dans un autre pays ou avec l'un de nos Centres mondiaux AMGE. Montrez vos résultats à votre éducateur et testez-les ensemble. Parmi les différentes méthodes, on compte : email, téléphone en ligne, appel vidéo et envoi d'une lettre à un groupe que vous avez trouvé en ligne.

Être en contact avec des personnes d'une autre culture est très enthousiasmant mais il est important de comprendre et respecter les différences qui existent entre vos vies. C'est tout aussi vrai lorsque vous vous connectez sur internet que si vous vous rencontriez en tête à tête. Faites des recherches sur leur culture et société et si vous voulez en apprendre davantage sur leur mode de vie, posez des questions sans porter de jugement. Si vous vous connectez en temps réel, n'oubliez pas de prendre en compte le décalage horaire.



**Prolongez l'exercice** – Ouvrez un compte sur SKYPE pour votre groupe et entrez en contact avec différents membres de l'AMGE de cette manière.



## SE CONNECTER POSITIVEMENT EN LIGNE

### 3 RÉSEAUX SOCIAUX

Les réseaux sociaux représentent une part importante de l'activité en ligne. Ils vous permettent de communiquer aisément avec vos amis et d'explorer un tas de nouveaux contenus comme les vidéos, photos et 'chats', tous réunis sur le même service internet.

- Vérifiez vos paramètres de confidentialité et demandez à l'un de vos amis ou à un membre de votre famille d'examiner votre profil afin de vous assurer de ne pas avoir posté des informations que vous ne souhaitez pas diffuser. Si vous consultez votre réseau social de manière quotidienne, vous pouvez très facilement passer à côté de certains points qu'il serait préférable de garder pour soi.
- Informez-vous sur la réputation numérique et la création sur Internet, vu l'importance majeure de ces deux points lors de l'utilisation des réseaux sociaux.
- Si vous avez moins de 13 ans, vous n'êtes pas censé avoir un compte Facebook.
- Si quelqu'un vous demande de devenir son « ami » sur Internet, ne répondez pas automatiquement « oui ». Connaissiez-vous réellement la personne ? Si ce n'est pas le cas, posez-vous la question afin de savoir si vous désirez réellement que cette personne ait accès à votre profil et à vos messages.



### 4 JOUEZ LA CARTE LOCALE

Il n'est pas uniquement question de connections mondiales. Internet peut être une façon fantastique d'entrer en contact avec votre communauté locale et de partager des opportunités. Mais que se passe-t-il si vous ne pouvez pas trouver les éléments dont vous avez besoin ? Recherchez la présence en ligne de votre communauté. Est-ce que cela pourrait être mieux ? Découvrez les opportunités offertes aux jeunes dans votre communauté et recherchez comment vous pourriez utiliser un portail internet, comme un site web ou une page Facebook pour faire passer un message et améliorer l'accès aux informations et opportunités de la communauté.



**Prolongez l'exercice** – Comment pourriez-vous utiliser internet pour donner le coup d'envoi d'un projet communautaire ? Certains groupes communautaires qui remportent un très vif succès utilisent internet pour mettre en relation les personnes qui recherchent un petit bout de terrain pour faire pousser leur propre nourriture avec des personnes qui ont des parcelles inutilisées autour de la communauté. D'autres l'utilisent pour faire de la publicité pour des articles qu'ils veulent recycler ou pour faire un échange de compétences. Par exemple, une personne qui peut enseigner l'espagnol cherche à rencontrer quelqu'un qui pourrait lui procurer des compétences de base en informatique. Qu'en serait-il d'un groupe chargé des actualités qui collecterait et partagerait les opportunités de volontariat pour les jeunes ? Faites un sondage auprès de votre communauté et identifiez un besoin auquel vous pensez pouvoir répondre grâce à internet.

## SE CONNECTER POSITIVEMENT EN LIGNE

### 5 AVENTURE EN LIGNE

L'un des plus grands atouts d'internet est qu'il offre des opportunités insoupçonnables. Quelle serait votre aventure ultime ? Peut-être un voyage vers un pays dont vous n'avez jamais entendu parler auparavant, ou un défi à haute performance pour stimuler votre rythme cardiaque ? Imaginez l'aventure parfaite, puis utilisez internet pour constituer un album virtuel de votre voyage avec des informations et des supports que vous trouverez en ligne. Partagez votre aventure avec votre groupe et exposez-la chez vous pour vous inspirer.



**Prolongez l'exercice** – Qu'advierait-il si votre rêve se réalisait et que vous puissiez réellement réserver votre séjour aventure ? Faites des recherches pour voir comment vous pourriez utiliser internet pour préparer l'itinéraire parfait, obtenir des informations privilégiées et débusquer la meilleure aubaine. Cependant, tous les bons plans ne sont pas tous bons à prendre, apprenez à déceler les arnaques ! Visitez les sites web sur la sécurité d'internet répertoriés au dos de ce kit, afin de connaître les conseils d'utilisation d'internet pour préparer des voyages.



### 6 LES BOUTIQUES EN LIGNE

Vous pouvez presque tout acheter en ligne. La plupart des produits peuvent être livrés à votre domicile, et les musiques, les films et les jeux que vous achetez sont directement téléchargeables sur votre terminal. Mais si vous cherchez le meilleur prix en ligne, mieux vaut vous méfier. Une grande quantité de sites Internet peuvent sembler offrir une occasion d'achat incroyable alors qu'ils n'ont d'autre but que de vous escroquer. Vous pourriez payer des produits qui ne vous seront jamais livrés ou vous pourriez recevoir des articles qui ne correspondent pas à votre commande. Il se peut également que les données de la carte de débit ou carte de crédit que vous avez utilisée lors de la commande soient utilisées de manière abusive. Même si vous demandez à vos parents d'acheter un article en votre nom, consultez le site avant de confirmer votre commande.

- Si vous achetez auprès de particuliers, comme par le biais d'eBay, vérifiez leur note de réputation.
- Consultez la police de confidentialité du vendeur et sa politique en matière de retour.
- Lorsque vous entrez les informations de votre carte de débit/crédit, vérifiez si la page de paiement est sécurisée. Le symbole d'un cadenas doit apparaître au bas à droite de la page du navigateur. Vous pouvez cliquer sur le cadenas pour vérifier si le vendeur est bien la personne qu'il prétend être et s'il possède un certificat de sécurité. Vérifiez également que l'adresse Internet commence bien par https:// (le "s" indique que la page est sécurisée).
- Ne faites pas d'achat d'articles proposés par un pourriel.
- Avant de payer, vérifiez les coûts additionnels demandés, comme les frais d'affranchissement élevés.



## SE CONNECTER POSITIVEMENT EN LIGNE

### 7 ENSEIGNEZ-LE !

Y a-t-il quelque chose que vous savez faire en ligne que des personnes plus âgées ne savent pas faire ? Parlez-en avec un adulte en qui vous avez confiance et cherchez à savoir ce qu'il leur plairait le plus de savoir faire en ligne et apprenez-leur à le faire.



**Prolongez l'exercice** – Créez un club internet au sein de votre communauté pour enseigner à des personnes âgées les compétences de base qui leur permettront de se connecter sur internet tout en se protégeant. Vous pouvez demander aux participants de faire un petit don pour la caisse de votre groupe.

### 8 LE MEILLEUR DU WEB

Il existe tellement de sites web formidables, qu'il n'est pas possible de tous les tester. Au lieu de cela, échangez vos informations avec vos amis ! En groupe, parlez de vos sites préférés, expliquez ce que vous y trouvez et pourquoi ils vous plaisent. Créez une carte visuelle des grands sites internet que votre groupe recommande et organisez-les par rubrique, par exemple : réseau social, écoute de musique, activités en extérieur ou jeux. Dans quelle mesure, selon vous, cette liste pourrait-elle aider quelqu'un qui recherche de nouveaux sites ou se connecte sur internet pour la première fois ?

### 9 RECHERCHE SÉCURISÉE

L'Internet constitue la plus grande bibliothèque qu'on puisse trouver à laquelle tout le monde peut contribuer. Toutefois, cela ne signifie pas que tout ce que vous trouvez sur Internet est fiable. En effet, le contenu n'est pas toujours rédigé par des experts. En outre, les individus ont des opinions diverses sur des sujets. Ces divergences affectent par conséquent leur manière de rédiger les articles. Comment vous assurer dès lors que vos recherches vous livrent des informations fiables ?

- Utilisez plus d'un mot pour décrire ce que vous recherchez. Par exemple, si vous souhaitez en savoir plus sur la culture musicale du Brésil, recherchez "Brésil danse musique culture", pour avoir des

informations plus spécifiques plutôt que d'inscrire uniquement "Brésil".

- Prenez le temps de réfléchir aux mots que vous allez inscrire avant de taper sur le bouton « recherche ». Les termes utilisés n'ont-ils pas d'autres significations qui pourraient conduire à des résultats non désirés ?
- Vérifiez votre information. Ce que vous trouvez sur Internet n'est pas toujours fiable, mieux vaut dès lors faire preuve d'intelligence lors de sa recherche et vérifier au moins trois sites différents pour confirmer l'information obtenue. N'oubliez pas non plus de consulter les livres ou de vous adresser à des personnes qui seraient susceptibles de connaître les informations que vous recherchez.
- Consultez régulièrement vos filtres de recherche, en particulier si vous recherchez des images, afin d'éviter tout matériel inapproprié. Vérifiez vos paramètres de recherche et sélectionnez les paramètres dont les niveaux de sécurité sont les plus élevés.
- Vous voulez retourner vers un site que vous avez consulté précédemment ? Veillez à référencer vos sites Internet favoris ou consultez votre historique pour vous assurer de retrouver la même page.
- Soyez attentifs à votre orthographe ! Une petite erreur de frappe dans votre recherche peut conduire à des résultats non désirés.
- Des logiciels de sécurité peuvent vous protéger contre les sites piratés. Pour assurer la sécurité de vos recherches, vous pouvez télécharger des outils de navigation ou utiliser les outils disponibles dans votre logiciel de sécurité visant à identifier les sites imposteurs. Certains montrent également les cotes d'appréciation des sites.

#### CONSEIL

Si quelque chose en ligne vous inquiète, parlez-en à un adulte en qui vous avez confiance.

## SE CONNECTER POSITIVEMENT EN LIGNE

### 11 SE METTRE AU PORTABLE

Surfer sur Internet ne se fait désormais plus uniquement sur les ordinateurs. Aujourd'hui, les téléphones portables, les tablettes numériques et les consoles de jeux portables vous permettent de vous connecter n'importe où. Comme pour les ordinateurs à la maison, il est tout aussi important d'utiliser ces matériels portables de manière intelligente. Voici quelques directives de base :

- Un texto peut très aisément être renvoyé et partagé avec d'autres personnes. Par conséquent, réfléchissez-y à deux fois avant d'envoyer un texto que vous n'aimeriez pas que d'autres personnes voient.
- La plupart des téléphones portables sont protégés par un mot de passe. Activez un mot de passe sur votre téléphone portable afin d'éviter que vos informations soient accessibles en cas de vol ou de perte de votre appareil. De plus, évitez que vos amis n'utilisent votre forfait de messagerie !
- Les virus pour la téléphonie mobile sont encore rares mais ils sont toutefois en circulation. Soyez dès lors vigilants et évitez de cliquer sur un lien inconnu ou de répondre à un texto non sollicité. Vérifiez si le logiciel de sécurité pour la marque de votre téléphone portable est à la hauteur de la tâche.
- Ne donnez jamais votre numéro de téléphone portable à une personne que vous avez rencontrée sur Internet et que vous ne connaissez pas en personne.
- Surveillez de près vos forfaits en minutes et en messagerie. Les frais d'utilisation d'un téléphone portable peuvent être coûteux. Cependant, vos parents seront plus enclins à vous laisser avoir un téléphone portable si vous recherchez les meilleurs tarifs et les compagnies les plus avantageuses en matière de téléphonie et si vous leur démontrez votre volonté à limiter les coûts au maximum. Si vous payez vous-mêmes vos notes de téléphone, cherchez toutes les économies que vous pouvez faire pour réduire le montant de vos factures. Réfléchissez à ce que vous pourriez faire avec cet argent économisé !



### 10 CHASSE AU TRÉSOR SMS

Comment utiliser la téléphonie mobile pour moderniser une activité traditionnelle ? Essayez d'organiser une chasse au trésor sms pour votre groupe. Explorez votre secteur et préparez des indices qu'un groupe peut suivre pour trouver des endroits précis, ainsi qu'une question sur chaque endroit à laquelle il ne peut répondre qu'une fois sur place. Faites partir le groupe avec un téléphone mobile et envoyez-lui par sms le premier indice et la première question. Lorsqu'il renvoie la réponse, envoyez-lui l'indice et la question du lieu suivant. En quoi l'utilisation du téléphone mobile a-t-elle modifié l'expérience ?



**Prolongez l'exercice** – Essayez d'autres manières d'utiliser la technologie mobile dans les activités. Pensez à incorporer des services comme Google maps, codes QR (un type de code barre que votre téléphone peut lire) et la Réalité Augmentée pour rendre les choses encore plus passionnantes ! Pourquoi devez-vous néanmoins réfléchir à deux fois avant d'utiliser des technologies qui permettent de vous localiser ?



## SE CONNECTER POSITIVEMENT EN LIGNE

### 12 BLOG SUR UN SUJET

Avez-vous déjà pensé à lancer un blog ? Les blogs sont une bonne manière de mettre en pratique vos talents créatifs par ex. à travers l'écriture et la photo. Cependant, il est important de prévoir à l'avance ce que vous mettrez dans votre blog et d'avoir une idée claire des informations que vous souhaitez voir apparaître sur votre blog ou que vous voulez garder pour vous. Les blogs qui rencontrent le plus de succès traitent de sujets qui intéressent les internautes. Que savez-vous ou bien sur quel sujet voulez-vous en savoir plus ? Établissez une liste de sujets de blogs sur lesquels il vous plairait d'écrire et échangez à ce sujet avec votre groupe. Qu'est-ce que vos amis trouveraient le plus intéressant à lire ? Créez un blog privé à partager avec vos amis et vos familles et actualisez-le pendant la durée d'un mandat.

### 13 BLOGUER

Les blogs sont des journaux de bord ou bloc-notes en ligne sur lesquels les visiteurs peuvent partager des opinions et exprimer leurs impressions et qui leur permettent de saisir des moments de leur vie au travers de textes, d'images et de vidéos. Vous pouvez opter pour la création d'un blog privé que vous partagerez avec des personnes que vous connaissez ou le rendre public. Les blogs sont une excellente façon de mettre en pratique vos compétences rédactionnelles et font appel à votre créativité. Vous pouvez également vous servir des blogs pour tisser des contacts directs avec des personnes qui partagent les mêmes intérêts que vous. Les blogs fonctionnent mieux s'ils concernent un sujet précis ou un intérêt particulier. Plutôt que de décrire votre petit-déjeuner, concentrez-vous davantage sur une chose qui vous tient à cœur. Plus le blog est spécifique, mieux ce sera ! Les sujets des blogs sont vastes et variés, allant de l'escalade à la cuisine japonaise, du kite surf à la collection d'éléphants. Vous avez également la possibilité d'écrire sur votre blog pour relater une expérience spécifique, comme un voyage à l'étranger ou vos cours de danse. Quel que soit le sujet de votre blog, veillez surtout à sécuriser votre blog.

#### Quelques conseils pour bloguer en toute sécurité

- Vérifiez vos paramètres de confidentialité et affichez un contenu en conséquence. Si votre blog est accessible aux personnes que vous connaissez, veillez à ne pas afficher des choses que vous n'aimeriez pas que ces personnes voient.

- Supprimez sur votre blog ou sur votre profil toutes les informations personnelles qui pourraient être utilisées pour vous identifier, comme vos noms complets, votre âge, votre lieu de résidence, vos numéros de téléphone et le nom de votre école.
- Apprenez à maîtriser les commentaires ou bloquez-les tout simplement. Soyez vigilants et contrôlez les commentaires postés sur votre blog afin d'éliminer ceux que vous jugez inappropriés.
- Rappelez-vous qu'à partir du moment où un élément est publié en ligne, il n'est plus possible de le retirer. Même si vous supprimez un billet, son contenu peut avoir été copié.
- Si un élément sur votre blog vous met mal à l'aise, tels que des commentaires affichés par d'autres personnes que vous n'appréciez pas, n'hésitez pas à en parler à un adulte de confiance.
- Ne commencez pas un blog par pur plaisir. Attendez d'avoir une idée précise du sujet que vous voulez traiter.
- Montrez votre blog à un adulte de confiance et demandez-lui de contrôler les affichages.



## SE CONNECTER POSITIVEMENT EN LIGNE

### 14 PROMO GROUPE

Comment feriez-vous la promotion du guidisme/scoutisme auprès de vos amis ? Réfléchissez à ce qui serait susceptible de leur plaire et faites une vidéo de promotion de votre groupe qui les encouragerait à s'engager. Vous pourriez par exemple leur présenter les activités en plein air auxquelles vous participez. Prévoyez d'utiliser internet pour partager votre vidéo avec votre public cible. Posez-vous les questions suivantes :

- Quel est votre public cible et comment pouvez-vous le trouver en ligne ?
- Comment suivre le nombre de personnes qui visionnent votre vidéo ?
- Quelles sont les coordonnées de contact que vous voulez partager et celles que vous voulez conserver à titre privé ?

Prenez en compte les questions de sécurité liées au chargement de la vidéo. Assurez-vous que votre projet de promotion de la vidéo assure votre sécurité, protège votre réputation et votre vie privée sur internet, et n'enfreint pas la législation sur les droits d'auteur, par exemple en utilisant des fichiers musicaux protégés. Après avoir réglé toutes ces questions, chargez votre vidéo et mettez votre plan en action. N'oubliez pas de partager le lien avec le groupe AMGE sur Facebook.



“ On estime que dans cinq ans, quelque 900 millions d'appareils électroniques pourraient être connectés à internet. Ce qui correspond au nombre de téléphones dans le monde. ”

### 15 REPORTAGE PHOTOS

Pouvez-vous prendre de bonnes photos ? Pourquoi ne pas faire un reportage avec des photos ? Décidez du message que vous voulez partager, prévoyez-le comme une série d'images, et prenez des photos qui, lorsqu'elles sont présentées dans un certain ordre, expriment ce que vous voulez exprimer. Vous pouvez prendre des photos avec une caméra numérique, votre téléphone ou d'autres périphériques mobiles.



**Prolongez l'exercice** – Chargez votre reportage sur internet en utilisant un service qui vous donne un contrôle privé, comme Flickr, Picasa, Photobucket ou un groupe Facebook. Ainsi, vous pouvez contrôler qui vous invitez à visionner votre reportage et le partager avec vos amis et votre famille. Apprenez comment marquer vos photos avec un filigrane qui peut empêcher des tiers de copier vos images. Essayez vous-même !



### 16 CRÉER POUR INTERNET

Parmi toutes les activités proposées, certaines vous invitent à créer et à télécharger un contenu sur Internet, comme des billets de blogs, des photos ou des vidéos. Vous souhaitez peut-être les partager publiquement, comme poster une vidéo promotionnelle sur YouTube, ou vous voudrez simplement les montrer à vos amis et à votre famille en téléchargeant ces publications sur un espace privé de partage en ligne et inviter les personnes à les visionner. Quelle que soit l'option choisie, dès que vous téléchargez votre contenu, vous concluez un accord avec le service Internet sur lequel vous vous connectez pour le téléchargement. Qu'il s'agisse de Facebook ou de YouTube, d'un site blog comme Tumblr ou d'un site de photos comme Flickr, à partir du moment où vous téléchargez votre contenu, vous acceptez les « conditions de service » ou les « conditions d'utilisation » du site en question, étant les réglementations d'un fournisseur de services en ligne auxquelles doivent se plier les utilisateurs. En d'autres termes, vous êtes supposé avoir lu les clauses en petits caractères avant de commencer à télécharger. Malheureusement, la plupart d'entre nous ne le fait pas.

Lorsque vous créez un contenu original, vous acquérez automatiquement des droits de propriété sur le contenu créé. Un contenu original est censé être votre propre création, à 100%. Il s'agira par exemple de l'enregistrement d'une chanson que vous chantez et que vous avez écrite, et non pas de chanter une chanson écrite par quelqu'un d'autre. Dans la majorité des services d'utilisation en ligne, vous conservez vos droits de propriété. Cependant, les services en ligne peuvent recourir à divers procédés pour utiliser votre contenu sans pour autant s'approprier vos droits de propriété. Ces façons de procéder sont incluses dans les conditions de service et conditions d'utilisation. En lisant attentivement les conditions d'utilisation du service que vous utilisez, vous noterez vraisemblablement une phrase qui ressemble à ceci : « En soumettant des contenus à notre Service, vous nous accordez une licence, dans le monde entier, non exclusive, gratuite d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de publication, d'affichage, de représentation publique ou de distribution publique desdits contenus. » Cela signifie que ce service peut tout faire avec votre contenu, même si celui-ci reste votre propriété. Ils peuvent le partager avec d'autres personnes dans le monde entier aussi longtemps qu'ils le souhaitent, ils peuvent le modifier, le publier sous toutes les formes,

le donner ou le vendre à d'autres entreprises qui feront de même. Ces conditions ne s'appliquent pas seulement aux vidéos et aux photos. Twitter, Facebook et d'autres réseaux incluent les mêmes droits dans leurs conditions écrites, de manière à pouvoir utiliser vos affichages et tweets. De même, certains services donnent des droits à "chaque utilisateur du Service" (toute personne possédant un compte sur le service en ligne, tel que vous). Cela signifie que n'importe qui peut utiliser ou partager vos contenus. Normalement, ces conditions ne s'appliquent que pour la durée de disponibilité de votre contenu sur le service. Si vous supprimez une vidéo ou une photo, le service n'a plus le droit de l'utiliser. Néanmoins, il est très difficile de savoir si des copies ont été conservées sur le serveur ou si une autre personne a copié votre travail et l'utilise pour son propre compte. Parfois, un service indique qu'il conserve ses droits sur vos contenus même si vous les supprimez. Ces clauses s'appliquent souvent aux contenus écrits, comme les billets et commentaires affichés. Ces directives constituent un bon début, pour vous assurer sur la façon dont un service en ligne utilise votre contenu, il convient de vérifier vous-mêmes les Conditions d'utilisation du site en question.



## ACTIVITÉS CONNECTÉ ET ÉCLAIRÉ

## SE PROTÉGER DES RISQUES EN LIGNE

### 1 FAITES VOTRE SHOW !

En petit groupe, choisissez trois conseils que vous trouvez important pour vous protéger en ligne. Créez une danse, une chanson ou un spectacle qui communique sur ces conseils et mettez-le en scène devant votre groupe.

Réfléchissez à la manière de rendre vos conseils de base faciles à comprendre pour de plus jeunes membres et faites votre représentation pour un groupe de plus jeunes enfants. Ensuite, échangez avec eux sur le message véhiculé par le spectacle.

**Prolongez l'exercice** – Enregistrez votre spectacle et chargez-le sur le canal YouTube de l'AMGE. N'oubliez pas de vérifier que toutes les personnes y figurant sont d'accord pour apparaître en ligne.

### 2 MOT DE PASSE PARFAIT

Échangez sur ce qui fait un bon mot de passe. Demandez à chaque membre du groupe d'écrire sur un papier un mot de passe imaginaire et de le placer dans un récipient. Ressortez les mots de passe, un par un, et demandez à chacun de lever la main pour signifier s'il paraît bon ou pas. Pouvez-vous deviner qui a écrit chacun des mots de passe ?

Recherchez les mots de passe les plus fréquemment utilisés en ligne. Pourquoi serait-ce une mauvaise idée de les utiliser ? Proposez des codes que vous pourriez utiliser pour créer de bons mots de passe comme 1) changer la première lettre d'un mois par le numéro de ce mois dans l'année, par ex. "avril" devient "4vril" ; 2) adapter une expression favorite, comme "toujours voir la vie du bon côté" et utiliser la première lettre de chaque mot, avec des majuscules pour les mots principaux, par ex. "TVIVdBC" ; ou 3) remplacer certaines lettres par des chiffres et des symboles par ex. en utilisant le chiffre "0" à la place de la lettre "o", ou "\$" à la place de "s".

### CONSEIL

Les restrictions relatives à l'âge ont pour but de vous empêcher d'accéder à des contenus que vous devriez pas voir. Si une page indique "18+", déconnectez-vous et dites-le à votre parent/responsable.



## SE PROTÉGER SOI-MÊME DES RISQUES EN LIGNE

### 3 LES BONNS MOTS DE PASSE

La clé pour créer un bon mot de passe est de trouver le juste équilibre entre un mot que vous n'aurez aucune difficulté à mémoriser mais qui est par contre difficile à deviner.

Pour vous assurer de choisir un bon mot de passe :

#### VEILLEZ À ...

- Choisir un mot de passe composé de huit caractères au minimum.
- Utiliser une combinaison de lettres, minuscules et majuscules, de chiffres et de symboles.
- Déconnectez-vous dès que vous cessez d'utiliser le service en ligne.

#### VEILLEZ À NE PAS ...

- Utiliser des mots simples qui se trouvent dans le dictionnaire.
- Inclure des informations personnelles tels que vos nom ou date d'anniversaire.
- Utiliser une numérotation ou dénomination évidente comme "12345678", "laisse-moi-entrer" ou "mot de passe".
- Utiliser le même mot de passe pour chaque compte. Utilisez des mots de passe uniques pour des comptes vraiment importants comme votre messagerie électronique et réseau social.
- Inscrire votre mot de passe sur des formulaires en ligne ou l'envoyer par courriel. Si vous recevez un message électronique en provenance d'un site Internet que vous consultez, qui vous demande votre mot de passe, il s'agit probablement d'une tentative d'hameçonnage, ne provenant pas nécessairement de ce site.
- Révéler votre mot de passe à vos amis. Ce n'est pas par manque de confiance en eux, il s'agit tout simplement d'une bonne habitude à prendre.
- Afficher votre mot de passe sur l'écran. Si vous devez l'écrire, assurez-vous de conserver le papier dans un lieu sûr et non visible. Vous pourriez par exemple le donner à vos parents. Ne stockez pas cette donnée sur votre ordinateur.

### 4 À CONSERVER À TITRE PRIVÉ

Un grand nombre de sites en ligne, comme les réseaux sociaux, les sites de stockage de données ou les jeux en ligne requièrent que vous créiez un compte et un profil personnel. Savez-vous combien de comptes vous avez ? Quand vous utiliserez internet au cours de la semaine à venir, répertoriez tous les sites en ligne sur lesquels vous avez un compte. "Marquez en vert" chacun des comptes de votre liste pour lesquels vous avez choisi des paramètres de confidentialité et créé un mot de passe sécurisé individuel.

#### CONSEIL

Vérifiez les paramètres de confidentialité des sites sur lesquels vous publiez des informations.



## SE PROTÉGER SOI-MÊME DES RISQUES EN LIGNE



### 5 COMBATTRE LES VIRUS

Qu'est-ce qu'un virus informatique ? Pourquoi certaines personnes créent-elles des virus ? Comment se propagent-ils ? De quelle manière pouvez-vous protéger votre ordinateur contre ces virus ? Invitez un professeur en TIC (technologies de l'information et de la communication) ou un spécialiste en informatique à venir devant votre groupe pour répondre à ces questions et expliquer comment un logiciel de sécurité sur internet fonctionne pour vous protéger. Vous pouvez également faire des recherches en ligne - <http://bit.ly/XUTVb> est un bon site pour débiter et présenter ce que vous avez appris devant votre groupe.

### 6 LOGICIELS MALVEILLANTS

Logiciel malveillant est le terme employé pour désigner les outils qu'utilisent les cybercriminels pour nuire aux informations stockées dans votre système informatique, pour vous inciter à entreprendre des actions que vous ne souhaitez pas et dérober vos informations personnelles. Les menaces des logiciels malveillants circulent depuis plus de 25 ans, et aujourd'hui, un nombre toujours croissant de programmes malveillants sont élaborés pour menacer

l'environnement mobile des réseaux sociaux et des téléphones portables. Voici quelques types de logiciels malveillants :

- Les logiciels espions ou mouchards sont des types de logiciels malveillants qui s'installent dans votre ordinateur dans le but de collecter et de transférer des informations à votre insu. Il est particulièrement difficile de détecter si des logiciels espions sont installés dans votre ordinateur. Il est donc vital de se munir de logiciels anti-espions et de sécurité visant à détecter les menaces, à désinfecter votre ordinateur et à le protéger contre toutes sortes d'intrusions.
  - Les virus informatiques sont des programmes qui sont capables de se répliquer pour se propager ensuite à d'autres ordinateurs, en s'insérant dans d'autres programmes et en endommageant les données qui y sont stockées afin d'empêcher leur bon fonctionnement.
  - Les chevaux de Troie sont une sorte de virus, excepté qu'ils sont conçus de telle manière qu'ils donnent l'apparence d'exécuter les actions que vous souhaitez, pour finalement exécuter, à votre insu, des instructions non désirées, comme copier et donner accès à votre ordinateur à une autre personne qui dérobera les informations stockées. Citons les exemples de téléchargements de jeux et d'économiseurs d'écrans gratuits. Vous téléchargez le fichier sans réaliser qu'il dissimule une fonction de malveillance.
  - Les vers informatiques sont une sorte de virus qui se propagent par eux-mêmes d'un ordinateur à l'autre en envoyant une copie d'eux-mêmes à des centaines de milliers d'ordinateurs. Par exemple, à toutes vos adresses électroniques enregistrées dans votre liste de contacts. Les vers peuvent être conçus de manière à permettre aux cybercriminels d'accéder à votre ordinateur et d'en prendre le contrôle à distance. Mais le plus souvent, ils utilisent simplement le système de mémoire ou la bande passante du réseau, détériorant ainsi les ordinateurs et les serveurs Internet.
- Comment pouvez-vous protéger votre ordinateur contre ces logiciels malveillants ?
- Vérifiez que votre système de sécurité Internet est bien activé et que les mises à jour se font automatiquement.
  - Veillez également à activer un pare-feu en plus de votre logiciel antivirus.
  - Soyez attentifs aux pourriels et aux sites Internet douteux. Ne cliquez pas, si vous n'avez pas confiance.



## SE PROTÉGER SOI-MÊME DES RISQUES EN LIGNE

### 7 AVATARS

Imaginez que vous rejoignez un réseau social. Au lieu d'exposer votre photo, créez un avatar : une image de bande dessinée qui vous représente. Accrochez les avatars de chacun tout autour du lieu de réunion, puis demandez à un leader d'appeler les noms des membres du groupe au hasard. Chacun doit essayer de deviner quelle image représente cette personne en allant se placer à côté de cette image. Les avatars sont une bonne manière d'exprimer votre propre identité en ligne sans divulguer d'informations vous concernant à des étrangers.

#### CONSEIL

Utilisez toujours un pseudo en ligne à la place de votre vrai nom et ne rendez pas public votre vrai nom si quelqu'un vous le demande.

“ Tout individu de moins de 13 ans n'est pas autorisé à avoir un compte Facebook ou à utiliser YouTube, pour garantir sa sécurité. ”



### 8 ANONYMAT FACE À L'ANONYMAT

Anonymat face à l'anonymat

Comment savez-vous si la personne que vous rencontrez en ligne est celle qu'elle prétend être ? Choisissez un de vos personnages favoris dans un livre ou un film et créez le profil de réseau social qui, selon vous, lui correspondrait avec les informations qu'il contiendrait. Créez une version papier de ce profil imaginaire ou mettez-le en scène, mais sans mentionner son nom ! Échangez les profils et essayez de deviner qui, votre ami(e) a choisi. Avez-vous l'impression d'en savoir plus sur cette personne maintenant ? Pouvez-vous vous fier aux informations que vous trouvez dans un profil en ligne ?



**Prolongez l'exercice** – Imaginez que votre ami(e) soit amenée à connaître votre personnage imaginaire par le biais d'un forum, et que vous craigniez qu'elle mente sur son identité. Quel avis donneriez-vous à votre ami(e) ? Imaginez les questions et les opinions que votre ami(e) pourrait avoir, puis écrivez-lui une lettre lui expliquant votre conseil, ou écrivez et mettez en scène un dialogue imaginaire avec un(e) ami(e) sur ce sujet. Comment pourriez-vous aider votre ami(e) et est-ce que vous le feriez d'une manière différente par rapport à l'aide que ses parents pourraient lui apporter ?

## SE PROTÉGER SOI-MÊME DES RISQUES EN LIGNE

### 9 PARTAGER LES APPRENTISSAGES

Par groupes, organisez une soirée d'information sur la sécurité internet pour un groupe de vos pairs ou de membres plus jeunes de votre communauté, comme un groupe de jeunes scouts/guides ou éclaireurs/éclaireuses. Déterminez ce qu'ils veulent savoir et prévoyez un ensemble d'activités ludiques qui introduisent des idées relatives à la sécurité sur internet sans utiliser d'ordinateur. Vous pouvez vous servir des activités et des jeux de ce kit ou bien créer les vôtres.

#### CONSEIL

Gardez votre mot de passe, et changez le souvent.

### 10 CYBERCRIMINALITÉ

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales qui sont commises sur le réseau Internet. La cybercriminalité est une pratique assez courante : à l'échelle mondiale, deux tiers des adultes ayant recours à l'Internet ont déjà vécu une expérience de cybercriminalité. On peut distinguer différents types de cybercriminalité, tels que :

- Pirater un ordinateur en effaçant des informations ou en endommageant le logiciel.
- Dérober des informations privées dans votre ordinateur ou sur votre réseau, comme votre adresse électronique ou vos données bancaires.
- Faire pression pour envoyer de l'argent, souvent au moyen de fausses annonces d'opportunité d'investissement, de prix à gagner ou de problèmes d'argent que connaîtrait une de vos connaissances résidant à l'étranger.
- Confirmer l'existence de votre adresse électronique pour vous envoyer plus de 'spam' sur cette adresse.
- Utiliser votre compte de messagerie (souvent à votre insu) pour envoyer des 'spam' dans le but de trouver les adresses électroniques de vos amis et des membres de votre famille.

- Vous identifier. En obtenant suffisamment d'informations personnelles sur votre compte, les cybercriminels peuvent profiter de vous dans la vie réelle, comme vous aborder dans un lieu que vous avez l'habitude de fréquenter ou usurper votre identité en ligne.

- Perturber ou effrayer sciemment une personne.
- Rappelez-vous que la cybercriminalité est une infraction au même titre que toute autre infraction hors ligne, commise dans la vie réelle. Si vous tombez sur quelque chose de dérangeant ou qui ne vous inspire pas confiance, ne répondez pas – bloquez l'adresse et parlez-en à un adulte de confiance.

### 11 SPAMS

Par groupes, recherchez les principales menaces en matière de sécurité internet : logiciel malveillant, hameçonnage et emails frauduleux. Planifiez et enregistrez une série de courts podcasts diffusant des informations sur ces menaces et la conduite à tenir en leur présence. Utilisez différentes méthodes pour rendre le sujet intéressant et attrayant comme des interviews fictives, "les meilleurs trucs" ou un reportage.

### 12 HAMEÇONNAGE

On parle d'hameçonnage, lorsqu'un email ou un site web essaie de vous tromper pour que vous transmettiez des informations privées comme des coordonnées bancaires. Un grand nombre d'emails frauduleux sont capturés par le filtre de spams dans votre messagerie, mais certains arrivent à s'introduire et il n'est pas toujours facile de faire la différence entre un email authentique et une tentative de hameçonnage. Essayez ce quiz pour apprendre comment repérer les emails présentant un risque : <http://bit.ly/zljxs7>

#### CONSEIL

Vous n'aimez pas ce que quelqu'un vous dit ? Bloquez-le !



### 13 FRAUDE PAR HAMEÇONNAGE ET PAR COURRIEL

Les courriels frauduleux sont des messages qui tentent de vous soutirer des informations ou qui vous incitent à verser de l'argent à une personne que vous ne connaissez pas. Ces messages racontent généralement une histoire dramatique, ou proposent des offres tentantes dans le but de vous faire réagir émotionnellement de sorte que vous suiviez les instructions indiquées sans réfléchir plus loin.

La fraude par hameçonnage désigne une technique d'escroquerie dont se servent des personnes pour voler des informations qui vous concernent en envoyant des courriels d'apparence officielle d'une organisation reconnue et de confiance. L'hameçonnage se fait généralement par voie de courriels mais peut également se produire par le biais d'appels téléphoniques et de textos. Les messages vous incitent à commettre des actes préjudiciables comme ouvrir une pièce jointe qui contient un virus, consulter des sites à risques ou donner vos données personnelles.

Afin de vous protéger des courriels frauduleux et des tentatives d'hameçonnage, soyez attentifs aux :

- Courriels en provenance de personnes que vous ne connaissez pas ou courriels non sollicités.
- Courriels envoyés par une personne figurant dans votre liste de contact mais qui est rédigé dans un style qui ne correspond pas à celui de votre ami ou amie, ou qui contient des instructions qui vous paraissent étranges, comme "J'ai trouvé cette super offre" ou "cliquez ici pour visionner la vidéo".
- Messages qui ne vous sont pas adressés

personnellement, qui s'adressent à vous en utilisant "Cher client" plutôt que votre nom.

- Messages qui ont recours à un langage dramatique ou qui racontent des histoires invraisemblables, comme vous offrir une grande somme d'argent, prétendre qu'un de vos amis est coincé à l'étranger et qu'il a besoin d'argent, ou qui disent que votre compte a été piraté ou que votre identité a été usurpée et qu'il faut que vous donniez votre mot de passe pour la récupérer.
- Tout courriel qui vous dit d'introduire votre mot de passe ou tout autre renseignement personnel, de vérifier votre compte ou de cliquer sur un lien. Courriels qui vous demande votre mot de passe, tout autre renseignement personnel, de vérifier votre compte ou de cliquer sur un lien.
- Les pièces jointes non sollicitées, comportant des noms et des types de fichiers de programme étranges, tels que des fichiers terminant par ".exe".

Il n'est pas toujours évident de repérer une tentative d'hameçonnage. Afin de veiller à votre sécurité, il est conseillé de suivre les règles de base suivantes :

- Ne jamais cliquer sur des liens dans les courriels. Au lieu de cela, entrez directement l'adresse du lien dans la barre d'adresse du navigateur.
- Si vous avez des doutes quant à l'authenticité d'un courriel que vous recevez, ne réagissez pas ou n'y répondez pas. S'il dit provenir d'un ami, contactez directement cet ami afin de vérifier s'il est bien l'auteur du message.
- En cas de doute, appuyez sur 'supprimer'.

#### CONSEIL

**Vous créez un profil sur un réseau social ou un forum ? Utilisez un avatar au lieu d'utiliser votre photo.**

### 14 DISCUSSION SUR LE WEB

Rédigez sur des morceaux de papier les questions ou les préoccupations que vous avez concernant l'utilisation d'internet. Mélangez-les, puis en groupe, prenez les papiers les uns après les autres et échangez autour. Rédigez la meilleure réponse à laquelle vous arrivez pour chaque problématique posée et reprenez l'ensemble dans une FAQ (foire aux questions). Partagez votre FAQ le plus largement possible, p. ex. dans votre école, auprès de vos familles et des groupes de votre communauté, ainsi que sur internet.

## ACTIVITÉS CONNECTÉ ET ÉCLAIRÉ

# FAIRE RESPECTER SES DROITS ET SA RÉPUTATION EN LIGNE



### 1 CYBERINTIMIDATION

Pourquoi, selon vous, des personnes peuvent se dire des choses méchantes en ligne ? Comment est-ce que cela arrive et que pouvez-vous faire pour arrêter cela ?

**Les plus jeunes** – Demandez à votre éducateur de passer des vidéos de mise en garde qui explorent la cyberintimidation et expliquent comment y mettre fin. Créez votre propre jeu pour sensibiliser à la cyberintimidation.



**Prolongez l'exercice** – Réalisez un film sur la cyberintimidation. Organisez une fête de lancement et partagez ce film avec les amis et les familles.

**Les plus âgé(e)s** – Menez un sondage au sujet de la cyberintimidation auprès de votre école ou groupe communautaire pour recueillir les opinions et expériences de vos pairs. Rédigez un rapport de synthèse, p. ex. sous forme d'affiche présentant des statistiques, dans le but de promouvoir un comportement positif en ligne. Pouvez-vous obtenir que votre rapport soit publié par votre école et/ou communauté locale, en ligne, hors ligne ou les deux ?





### CONSEIL

Ne communiquez à personne votre âge, vos coordonnées, adresse ou nom de votre établissement scolaire.

## 2 LE HARCÈLEMENT EN LIGNE OU CYBER-HARCÈLEMENT

Nous parlons de cyber-harcèlement lorsqu'un individu utilise la technologie pour sciemment faire du tort à une autre personne et de manière répétitive. Il se peut qu'une personne n'ait pas d'intention malveillante à priori et ne souhaite faire qu'une simple plaisanterie, cependant, le mal est fait à partir du moment où un individu a été blessé. Personne n'est à l'abri et les victimes de ce préjudice ressentent un sentiment de solitude et d'insécurité. Le cyber-harcèlement peut se traduire sous diverses formes :

- Exclure une personne des conversations en ligne
- Etiqueter des images de manière inappropriée
- Envoyer des messages texto et des courriels injurieux ou désobligeants
- Poster des images ou des messages irrespectueux sur les sites des réseaux sociaux
- Imiter d'autres personnes en ligne.

Personne ne souhaite être traité de manière malveillante, que ce soit physiquement ou virtuellement. Le harcèlement en ligne peut se révéler particulièrement déstabilisant pour un individu dans la mesure où il peut se produire à n'importe quel moment ou à n'importe quel endroit. Il suffit à un harceleur d'avoir un accès à Internet ou à un téléphone portable pour atteindre sa cible. Si cela se passe dans un lieu public, tel qu'un réseau social, plusieurs personnes peuvent être impliquées. La personne à l'origine du harcèlement en ligne pourra opérer dans l'anonymat et en sécurité, étant donné la difficulté de définir exactement d'où part la mauvaise action.

### Que faire si cela m'arrive ?

- Ne répondez pas. Changez vos paramètres de confidentialité et bloquez la personne responsable.
- S'il existe un lien "signaler un abus", cliquez dessus.
- Sauvegardez tous les courriels, textos et conversations.
- Parlez du problème à une personne de confiance, un bon ami ou un membre de la famille.
- Ne partez pas du principe qu'on ne peut rien y faire. Le cyber-harcèlement est considéré comme un crime dans de nombreux pays, et la maltraitance fait souvent l'objet de poursuites judiciaires.
- Si la personne à l'origine de ces actions de malveillance fréquente la même école que vous ou échange des messages cruels avec d'autres camarades de classe, parlez-en à un professeur en qui vous avez confiance et demandez-lui conseil. L'école pourrait avoir des outils appropriés susceptibles de vous aider.

### Que faut-il faire si cela arrive à un de mes amis ?

Si vous connaissez une personne qui est victime de harcèlement en ligne, vous pouvez l'aider.

- Ne participez pas. En diffusant des messages injurieux ou des photos irrespectueuses, vous participez à l'acte de malveillance, sans en être pour autant l'initiateur.
- Parlez à votre ami(e) et faites en sorte qu'il/elle sache que vous le/la soutenez et qu'il/elle n'est pas seul(e).
- Parlez-en à un adulte de confiance en relatant les faits.

3

### CYBER-AMIS

Avoir de bons amis, c'est important pour tout le monde. Comment pouvez-vous être un (une) bon(ne) ami(e) dans votre vie quotidienne et sur internet ?



Échangez sur le lien qui peut exister entre la manière dont vous traitez vos amis sur le net et vos liens d'amitié au quotidien. Réfléchissez à trois façons simples d'être un(e) bon(ne) ami(e) sur le net, puis créez une image illustrant vos idées, comme une promesse que vous faites à vos amis. Faites des échanges de promesses au sein de votre groupe et exposez chez vous la promesse d'un(e) ami(e).



Une fois par jour au cours de la semaine à venir, faites un effort pour publier un message positif en ligne, pour que les autres se sentent bien dans leur peau, dans le cadre de vos activités habituelles sur le réseau social.



4

### ANONYME EN LIGNE ?

Collectez de nouveaux témoignages au sujet de la censure et de l'anonymat en ligne.

Quand l'anonymat en ligne est-il une bonne chose et quand peut-il être une mauvaise idée ? Pensez-vous que c'est une bonne chose que des contenus en ligne soient censurés ?

Partagez-vous en deux équipes et organisez un débat sur la censure ou l'anonymat en ligne, avec une équipe argumentant le "pour" et l'autre le "contre". Faites des recherches sur le sujet et ouvrez le débat en invitant vos amis et vos familles à y participer.

### ASTUCE

Si vous voulez transférer un email, rappelez-vous que vous ne pouvez pas contrôler avec qui cet email sera partagé une fois que vous aurez appuyé sur "envoyer". Protégez les adresses emails de vos amis en utilisant la "copie carbone invisible" ou "cci". En savoir plus sur <http://bbc.in/iXeSov>.



### 5 CONNAÎTRE VOS PISTES DE RECHERCHE

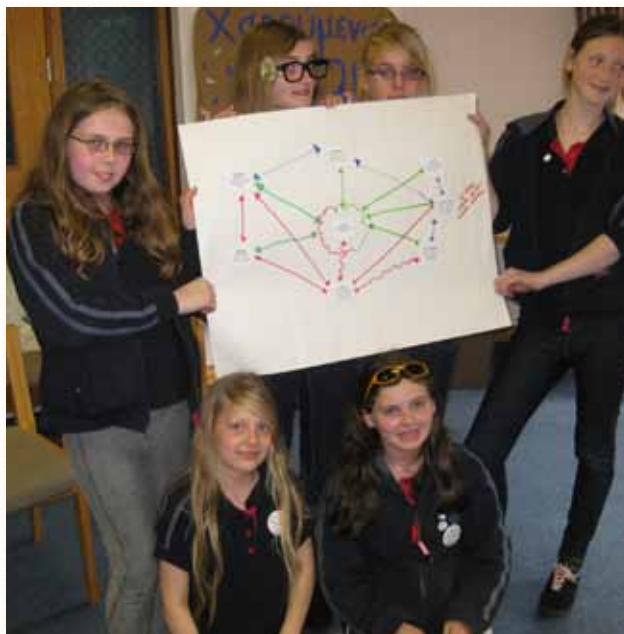
Il est facile d'imaginer que lorsque nous sommes en ligne, nous gardons l'anonymat. Or, ce n'est pas le cas. Vous laissez une trace à chaque fois que vous vous connectez sur Internet. Ce n'est pas grave en soi à partir du moment où les informations qui vous concernent sont positives et ne dévoilent aucun élément de votre vie privée. Tout ce que vous ou une autre personne poste sur Internet à votre sujet s'ajoute à votre « empreinte numérique ». Voici quelques conseils qui vous aideront à mieux comprendre la trace que vous laissez sur Internet.

- Lancez une recherche sur vous en tapant votre nom sur Google et voyez ce qui apparaît. Si un grand nombre de personnes portent le même nom que le vôtre, ajoutez quelques termes plus spécifiques, tels que votre pays ou la ville dans laquelle vous vivez.
- Consultez l'historique de votre navigateur de site Internet pour vérifier les sites que vous avez consultés dans le passé.
- Un numéro spécifique est attribué à chaque dispositif afin de l'identifier à chaque branchement de l'appareil sur Internet. Il s'agit de l'adresse IP. Sans ce numéro d'identification, il vous serait impossible de recevoir des informations des sites Internet. Au besoin, les sites Internet et les organisations, comme la police, peuvent utiliser les adresses IP dans le but d'identifier celui qui a exécuté une action spécifique en ligne.

- Aucun téléchargement sur Internet ne sera jamais réellement supprimé. Toute personne ayant aperçu votre publication ou image affichée sur Internet peut en avoir fait une copie sur son propre ordinateur. Les informations personnelles sont recueillies et archivées par les entreprises qui les utiliseront pour vendre leurs produits. Les individus qui souhaitent en savoir plus à votre sujet peuvent apprendre énormément de choses en faisant des recherches sur Internet. Soyez donc vigilants à ce que vous tenez à partager !
- Vous voulez voir ce que vos amis aperçoivent quand ils consultent votre profil sur Facebook ? Allez à la page des paramètres du compte > Paramètres de confidentialité > Visualiser les paramètres > Aperçu de mon profil.
- Si vous n'aimez pas ce que vous découvrez, vérifiez tout d'abord s'il est possible de supprimer un contenu, tout en gardant à l'esprit que même si vous supprimez tout affichage ou photographie embarrassante, vous ne serez jamais certain de la disparition complète de cet élément sur le réseau Internet. La prochaine étape sera de créer un contenu positif à votre sujet sur Internet, un contenu sécurisé qui ne dévoile aucune information personnelle à votre sujet, qui vous présente sous un jour positif, afin d'encourager des résultats de recherche positifs, qui vous pousseront en tête de liste de Google.

### CONSEIL

Demandez l'avis d'un parent/responsable avant de télécharger quoi que ce soit. Les téléchargements peuvent contenir des logiciels malveillants susceptibles de créer des dommages sur votre ordinateur.



### 6 ÉTUDIEZ INTELLIGEMMENT

Marre des devoirs qui n'en finissent plus ? Il peut être tentant de trouver des informations en ligne sur votre sujet et de faire un copier-coller. Le problème est que vous serez rapidement repéré par votre professeur et que les informations repérées sur le web ne sont pas forcément fiables.

Voyez par vous-même. Mettez-vous en binômes. Une personne trouve quelques paragraphes de texte en ligne, fait un copier-coller dans un document word et l'envoie par email à l'autre personne qui essaie de retrouver le texte source.



### ASTUCE

Ne cliquez jamais sur une fenêtre pop-up, même si c'est écrit "fermer" ou "annuler". Utilisez toujours la croix rouge pour vous en débarrasser.

### 7 BONNE RÉPUTATION

Votre réputation en ligne est l'image que vous véhiculez à travers vos actions en ligne. Elle recouvre les photos que vous chargez, les posts que vous publiez, les emails ou les textos que vous envoyez et les commentaires que vous faites dans les salons de discussions, sur les services de messagerie, dans les forums ou sur les sites web. Une fois que vous avez mis en ligne des informations, elles y restent. Même si vous supprimez quelque chose que vous avez publié ou chargé, quelqu'un peut déjà l'avoir copié.

Imaginez que vous postuliez pour un emploi ou une formation. Écrivez cinq points que vous souhaiteriez exprimer sur vous-même dans votre demande. Puis regardez votre profil de réseau social et recherchez votre nom sur internet. Quels sont, selon vous, les cinq principaux aspects qu'expriment vos profils en ligne ? Que pouvez-vous faire pour vous assurer que la personne qui vous proposera un emploi ou une formation verra ce que vous voudriez qu'elle voit si elle fait une recherche en ligne sur votre nom ?





### 8 RÉPUTATION NUMÉRIQUE

Ne soyez pas de ceux qui ont des regrets.

Comment réagiriez-vous si la blague que vous aviez faite sur votre professeur aboutissait brusquement sur son bureau ? Ou cette photo où vous apparaissez faisant la fête ? Comment réagiriez-vous dans cinq ans quand votre nouveau patron tombera sur cette photo lorsqu'il cherchera des informations qui vous concerne ? Votre réputation numérique se construit autour des opinions que les autres partagent à votre propos à travers vos actes affichés en ligne, et contrairement à ce que vous pourriez penser et dire à haute voix, Internet n'oublie pas ce qui a été publié. Quelle image voulez-vous donner de vous-même ? Vous ne vous en rendez peut-être pas bien compte, mais c'est vous qui contrôlez tout cela. Voici quelques conseils pour garder une réputation intacte :

- Consultez vos paramètres de confidentialité sur les réseaux sociaux pour empêcher toute personne étrangère de trouver des informations à votre sujet.
- Privilégiez une approche positive et évitez toute connotation négative. Réfléchissez à la façon dont réagirait une personne que vous respectez si elle voyait le billet ou la photo que vous avez postés sur Internet.
- Si un de vos amis vous identifie sur une photo en vous dépeignant sous un jour négatif, supprimez l'identification et demandez-lui de retirer la photo.

- Lorsque vous configurez votre profil sur un réseau social, n'utilisez pas votre nom complet.
- Soyez attentifs à l'orthographe et à la grammaire. Certaines entreprises voient les fautes d'orthographe et les erreurs de grammaire comme un signe d'immaturité et de faiblesse en matière de compétences en communication.
- Souvenez-vous que l'affichage est permanent et qu'il vaut mieux réfléchir à deux fois avant de poster quelque chose sur Internet.
- Surveillez votre réputation numérique en recherchant votre nom sur Internet et demandez à supprimer ce que vous ne souhaitez pas voir apparaître sur vous en ligne.
- Si vous souhaitez résoudre un problème une bonne fois pour toutes, n'hésitez pas à en parler face à face avec la personne concernée.
- Si vous faites des erreurs, remettez les choses au clair le plus rapidement possible. Les informations se propagent à une vitesse telle que si vous voulez limiter les conséquences d'un affichage désagréable ou d'une photo embarrassante, il faut les supprimer aussi vite que possible. Vous devez des excuses à quelqu'un ? Sachez qu'une personne y gagne toujours à assumer la responsabilité de ses erreurs.



### 9 COMBLER LE FOSSÉ

Lorsque vous êtes confronté(e) à un problème en ligne, on vous conseillera souvent d'en parler à un adulte en qui vous avez confiance comme un parent/responsable, enseignant ou éducateur de groupe communautaire. Cependant, vous pouvez ne pas souhaiter le faire. En petits groupes, lancez des idées sur les problèmes en ligne dont vous avez entendu parler ou que vous avez expérimentés. Puis décidez quels sont les problèmes dont vous devriez vous ouvrir à un adulte ou les situations dans lesquelles le soutien d'un adulte vous aiderait.

Vous sentez-vous à l'aise pour parler à votre parent/responsable de ce que vous faites en ligne ? Réfléchissez à une action que vous pourriez mener et qui serait susceptible de vous aider, vous et votre parent/responsable à parler plus ouvertement de votre utilisation d'internet. Il pourrait s'agir de lui faire faire une visite guidée de vos sites web favoris, lui faire voir comment réaliser telle action en ligne, ou conclure un accord sur l'utilisation d'internet qui serait signé par les deux parties.

### 10 TEMPS PASSÉ EN LIGNE

Combien de temps pensez-vous passer en ligne chaque semaine ? Rédigez une liste des activités principales que vous réalisez en ligne, comme lire vos emails, écouter de la musique, jouer à des jeux ou vous connecter sur les réseaux sociaux. Au regard de chaque activité, inscrivez le nombre d'heures et de minutes que vous pensez y passer chaque semaine. Pour la semaine à venir, notez le temps que vous passez pour chaque activité de votre liste et comparez avec vos estimations. Y a-t-il une différence ? Selon vous, combien de temps devriez-vous passer en ligne par semaine ?

Avec votre groupe, réalisez une horloge avec des aiguilles. Avec votre parent/responsable, mettez-vous d'accord sur un nombre d'heures à passer en ligne par semaine qui paraît approprié et inscrivez ce nombre d'heures sur l'horloge. En début de semaine, mettez l'horloge à "0". Chaque fois que vous vous connectez, avancez l'aiguille de votre horloge pour représenter le temps que vous avez passé en ligne. Est-ce facile de gérer votre temps sur la semaine ?



### 11 EMPREINTE NUMÉRIQUE

Avez-vous une idée de la quantité de contenus que vous mettez en ligne ? Esquissez une large empreinte sur un morceau de papier et tout au long de la semaine, chaque fois que vous publiez ou chargez un contenu en ligne, inscrivez-le sur votre empreinte. Ne décrivez pas en détails, inscrivez juste p. ex. "mise à jour de mon statut", "chat avec Claire pendant une demie heure sur Messenger", "transfert de 20 photos de ma fête d'anniversaire sur Facebook". Échangez sur vos empreintes sur votre lieu de réunion. Combien de temps vous a-t-il fallu pour remplir votre empreinte ? Imaginez le nombre d'empreintes que vous pourriez remplir sur une année. Qu'en ressentez-vous ?

“ Un ordinateur coûte l'équivalent d'un mois de salaire pour un Américain moyen, à comparer avec huit années de revenus pour un Bangladais moyen. ”



### 12 SUR LA CARTE

Vous êtes-vous jamais demandé comment votre téléphone portable pouvait vous localiser sur une carte ?

Les services de localisation sont très efficaces. Ils vous indiquent où se trouvent les arrêts de bus ou les distributeurs de billets les plus proches, ils vous aident à retrouver votre chemin. De plus, en cas de problème, les services d'urgence ont la possibilité d'utiliser le signal émis par votre portable pour vous retrouver, et en cas de perte de votre appareil, vous pouvez vous servir du signal pour vous aider à le repérer. Mais d'autres personnes peuvent également se servir des services de localisation pour vous repérer ; il peut s'agir de personnes que vous ne connaissez pas ou dont vous vous méfiez.

Comment cela marche-t-il ? Il existe principalement trois façons de localiser un appareil portable :

- GPS (Global Positioning System) ou système de positionnement global. Si votre téléphone dispose d'un récepteur GPS, il peut recevoir des signaux en provenance des satellites en orbite autour de la terre. Les satellites émettent des signaux et les GPS utilisent la distance entre les satellites et le récepteur (votre téléphone) pour calculer votre position.
- GSM (Global Systems Mobile) ou système mondial de communication mobile, fonctionne de la même

manière, excepté qu'il utilise les signaux émis depuis les pylônes de téléphonie mobile et non des satellites. Si votre téléphone permet d'accéder à Internet, il dispose probablement d'un récepteur GPS. Dans le cas contraire, votre téléphone portable peut toujours être localisé en utilisant la technologie du GSM, pour autant qu'il soit allumé.

- Enfin, votre portable peut être localisé par le biais des différents points d'accès Internet disponibles pour votre téléphone, tels que le réseau Internet à votre domicile ou les bornes Wi-Fi.

Si votre téléphone est équipé pour l'accès informatique, il combine probablement ces trois méthodes qui permettent de vous localiser rapidement et avec précision. Dès que votre dispositif détermine votre emplacement géographique, il existe diverses façons pour faire partager cette indication en ligne. Vous pouvez vous "connecter" sur Facebook pour indiquer votre position à tout moment. Il existe également un tas d'autres applications mobiles et services en ligne qui demandent de connaître votre localisation. Vous avez toutefois la possibilité de contrôler la ou les personnes qui verront cette information. Il n'est pas bon d'informer des étrangers sur l'endroit où vous vous trouvez, alors que vous ne savez même pas qui sont ces personnes. Il convient dès lors de bien réfléchir avant d'utiliser ces services de localisation, et en particulier si ceux-ci rendent l'information publique.

“ Il a fallu 38 ans aux diffuseurs radio pour atteindre une audience de 50 millions de personnes, 13 ans à la télévision et seulement 4 ans à internet. ”



### 13 TELECHARGER EN TOUTE CONSCIENCE

Il existe quantité de contenus numériques fantastiques sur internet que vous pouvez télécharger, comme des photos, de la musique et des films. Cependant, il est important de vérifier que vous n'utilisez que des sites légaux et que vous ne prenez pas quelque chose qui possède des droits d'auteur sans les payer. Le téléchargement de fichiers illicites s'appelle du piratage.

Par groupes, imaginez-vous dans la peau d'un chanteur dont la musique est volée par le piratage en ligne. Écrivez une chanson ou un message rap à l'adresse des personnes qui ont volé votre musique, expliquant ce que vous ressentez.

#### CONSEIL

Réfléchissez avant de publier un post. Une fois que vous avez cliqué sur "envoyer", il est parti pour toujours et vous ne pouvez pas contrôler qui le regarde.

“ 48 heures de vidéos sont chargées sur YouTube toutes les minutes, c'est presque l'équivalent de huit années de contenus chargés chaque jour, et plus de trois milliards de vidéos sont visionnées quotidiennement. ”



## SE RESPECTER VOS DROITS, VALEURS ET RÉPUTATION EN LIGNE

14

OK pour le téléchargement ?

Les opérations de streaming et de téléchargement de films et de musique

constituent une part importante de l'activité en ligne. Un grand nombre de sites Internet vous proposent un libre accès à de très bons et nouveaux matériels. Mais ce n'est malheureusement pas toujours légal.

C'est une question de droits d'auteur. Si vous créez quelque chose d'original, vous acquérez le droit sur ce contenu et vous êtes en droit de contrôler qui l'utilise, le modifie ou le copie. Les artistes gagnent leur vie grâce aux droits d'auteur, qui représentent la somme d'argent qu'ils perçoivent chaque fois que quelqu'un achète un exemplaire de leur travail, que ce soit sous la forme d'un CD/DVD, de tickets de concert ou de cinéma, ou d'une version numérique. Si vous téléchargez quelque chose illégalement, vous vous appropriez ce quelque chose sans demander l'autorisation du propriétaire.

Vous devez donc faire un choix. Où vous êtes-vous procuré votre média et qu'est ce que cela signifie pour vous ?

### Quelques éléments de réflexion :

- Le risque d'infecter votre ordinateur avec des logiciels malveillants est bien plus élevé si vous téléchargez des dossiers illégalement. Le matériel piraté représente une opportunité idéale pour les cybercriminels. Si un dossier contient un logiciel malveillant et endommage votre ordinateur ou dérobe une information, vous êtes peu susceptible d'en faire état parce que cela suppose que vous devrez admettre avoir enfreint la loi.
- Il est vrai que les entreprises qui gèrent les artistes, comme les maisons de disques, gagnent bien plus d'argent que les artistes. Cependant, ces accords lient les artistes à leur société de disques, et n'ont rien à voir avec nos choix de payer pour le contenu que nous souhaitons ou d'essayer de l'obtenir gratuitement.
- Nombreux sont les artistes qui s'insurgent contre le fait que tout leur travail de création peut être téléchargé pour rien. Les personnes qui téléchargent des copies pirates du travail d'un artiste ne tiennent pas compte des sentiments de l'artiste.
- Si vous utilisez des services illégaux, vous enfreignez la loi et vous vous exposez à des risques de sanction pénale. Vous pensez peut-être que les risques de se faire prendre sont minimes. Si toutefois vous deviez

être la personne sanctionnée, vous seriez traduite en justice, avec une peine pouvant avoir de lourdes conséquences, qui affecteraient gravement votre avenir : des amendes énormes, l'interdiction d'utiliser l'Internet, un casier judiciaire, et éventuellement une peine de prison.

- Contrairement aux idées reçues, copier des informations équivaut à les voler à son auteur. C'est le cas par exemple, lorsqu'on utilise la chanson d'un groupe ou une musique de film sans l'acheter. C'est ainsi que fonctionne l'industrie créative, et que les artistes se rémunèrent.
- Les copies pirates sont souvent de moins bonne qualité que les copies que vous pouvez acquérir de manière légale.

Cela ne signifie pas que vous devez payer une fortune pour acquérir des musiques ou des films. Il existe plusieurs excellentes façons de se procurer légalement des contenus sans dépenser nécessairement beaucoup d'argent.

- Discutez avec vos parents/ tuteurs sur la façon d'accéder aux médias de manière légale. La plupart des services de téléchargement payants demandent de payer par carte de crédit, mais il existe des services qui proposent des options de cotisation familiale ou de prépaiement afin que vos parents/tuteurs puissent intervenir et trouver une solution. Les sites les plus connus sont iTunes, Spotify, Lovefilm et Netflix.
- Vous vous sentez une âme avant-gardiste ? Au lieu d'acheter le tout dernier album à la mode, essayez de trouver des groupes de musique qui seront peut-être les nouvelles prochaines grandes stars. Les artistes qui souhaitent diffuser plus largement leur travail utilisent de plus en plus une licence Creative Commons. En d'autres termes, ils conservent leurs droits mais donnent au public l'accès gratuit à leur musique. Consultez les sites comme [www.jamendo.com](http://www.jamendo.com) pour explorer en toute légalité quelques nouveaux morceaux de musique.
- Essayez également d'écouter la musique par le biais de l'Internet. Des centaines de radios sont accessibles, gratuitement. Commencez par les sites de stations de radio nationales que vous connaissez avant d'explorer d'autres options sécurisées.

## CHOISISSEZ VOTRE PROPRE SÉCURITÉ D'ABORD !

Maintenant que vous avez une bonne idée de la manière dont vous pouvez tirer le meilleur parti d'Internet et vous protéger en même temps, marquez une pause et repensez à ce que vous avez appris. Comment pouvez-vous mettre en application ces idées dans votre propre vie ? Imaginez que vous vous promettiez de vous protéger en ligne. Comment la formulerez-vous ?

Par exemple...

“ Je marquerai une pause et réfléchirai avant de publier des informations sur Internet ”

“ Je parlerais à un adulte en qui j'ai confiance si quelque chose qui me chagrine m'arrive en ligne ”

“ Je serai prudent(e) lorsque j'ouvrirai mes mails ou cliquerai sur des liens et je bloquerai tout ce qui ne me semblera pas sûr. ”



## MON ENGAGEMENT “SÉCURITÉ SUR INTERNET”

Prenez vos principaux engagements et inscrivez les ci-dessous. Imprimez-les et discutez-en avec votre famille. Gardez-les près de votre ordinateur pour vous souvenir de ce que vous avez appris.

MON ENGAGEMENT SECURITE SUR INTERNET

Je veux me protéger en ligne et tirer le meilleur parti d'internet. Pour ce faire, je m'engage à :

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

Signature..... Date.....

## RESSOURCES

### SÉCURITÉ INTERNET

[www.kidsmart.org.uk](http://www.kidsmart.org.uk)

Rapport EU Kids Online :  
[www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx)

Restez maître de votre espace – Cyber-livre pour les adolescents  
<http://www.microsoft.com/download/en/details.aspx?id=1522>.

[www.childnet-int.org](http://www.childnet-int.org)

[www.google.co.uk/goodtoknow](http://www.google.co.uk/goodtoknow)

<http://staysafeonline.org/>

[www.netsmartz.org](http://www.netsmartz.org)

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

<http://www.digizen.org/>

<http://www.saferinternetday.org>

<https://www.facebook.com/help/privacy>

<http://www.bbc.co.uk/webwise/>

Commission nationale de l'informatique et des libertés (portail jeunes) :  
[www.jeunes.cnil.fr](http://www.jeunes.cnil.fr) et [www.youtube.com/lacnil](http://www.youtube.com/lacnil)  
(sur l'impact de la diffusion des images sur les personnes filmées : la fin de l'histoire change en fonction du partage ou non de la vidéo)

Voir aussi l'application smartphone de la CNIL, destinée aux jeunes « Pour apprendre à rester net sur le web »

Des conseils utiles sur la sécurité des données sur le réseau social facebook :  
[www.facebook.com/safety](http://www.facebook.com/safety)

Le site du réseau européen Insafe (anglais) :  
<http://www.saferinternet.org/web/guest/home>

Et son kit d'animation “Apprendre en s'amusant, l'univers en ligne” (pour les 4-8 ans) :  
<http://goo.gl/8Lfef>

Pour voir des vidéos vous montrant comment vérifier certains paramètres clés de sécurité et de confidentialité :  
[www.kidsmart.org.uk/skills-school/](http://www.kidsmart.org.uk/skills-school/)

### ALLER PLUS LOIN

[www.wagggsworld.org](http://www.wagggsworld.org)

<http://www.eurodesk.org.uk/>

[http://www.coe.int/t/dg4/youth/default\\_en.asp](http://www.coe.int/t/dg4/youth/default_en.asp)

<http://www.ted.com/>

<http://www.howstuffworks.com/>

<http://www.googleartproject.com/>

<http://www.unwomen.org/>

<http://www.youthforum.org/>

<http://www.paneuyouth.eu/web/youth>

Le site d'Internet Sans Crainte, programme national de sensibilisation des jeunes aux bons usages de l'internet :  
<http://www.internetsanscrainte.fr/accueil>

Et ses kits d'animations :

- Vinz et lou :  
<http://www.internetsanscrainte.fr/le-coin-des-juniors/pseudo-007>
- Le jeu « 2025 ex machina » sur la pratique des jeunes sur internet :  
<http://www.internetsanscrainte.fr/espace-jeunes/accueil>

Jeu-questionnaire sur les usages et dangers d'internet pour les adolescents :  
<http://www.adonautes.fr/>



**Antivirus** – logiciel conçu pour détecter et détruire des virus informatiques.

**Avatars** – Images graphiques utilisées pour représenter des utilisateurs dans des espaces en ligne. Elles peuvent être ou ne pas être des représentations authentiques des personnes qui les utilisent.

**Bande passante** – quantité maximale d’informations qui peuvent être transmises par un canal, comme une connexion internet.

**Blogguer** – Faire partager vos opinions et vos expériences sous forme d’un journal en ligne, dans lequel les lecteurs peuvent apporter des commentaires par des posts.

**Stockage dans le Cloud** – Service qui permet de sauvegarder des données en les transférant par internet sur un système de stockage hors site dont la maintenance est assurée par un tiers.

**Virus informatique** – programme informatique capable de se reproduire et d’endommager des fichiers ou des programmes sur l’ordinateur.

**Cyberintimidation** – utilisation des technologies de l’information et de la communication pour servir de support à un comportement délibéré, répété et hostile de la part d’un individu ou d’un groupe qui vise à nuire à autrui.

**Cybercriminalité** – tout crime qui fait intervenir un ordinateur et un réseau.

**Empreinte numérique** – La somme des informations que les personnes laissent en ligne.

**Réputation numérique** – Opinion que l’on a de vous sur la base des informations visibles vous concernant sur internet.

**Filigrane numérique** – un modèle inséré dans une image numérique, un fichier audio ou vidéo contenant des informations sur les droits d’auteur et le nom du créateur du fichier.

**Téléchargement** – transférer un fichier ou un programme à partir d’un système distant vers un ordinateur local ou un périphérique mobile.

**Facebook** – plus vaste réseau social sur internet. Il permet aux utilisateurs de créer des profils personnels et de se connecter avec des amis.

**Geo data** – données numériques représentant une localisation géographique.

**GPS** (Système de localisation mondial) – système de navigation faisant appel à des satellites et des ordinateurs pour calculer la localisation d’un dispositif récepteur. Un grand nombre de téléphones mobiles contiennent des récepteurs GPS.

**GSM** (Système mondial pour périphériques mobiles) – norme pour communications mobiles, utilisée par la plupart des services de téléphonie mobile dans le monde. Il peut aussi être utilisé pour identifier la localisation d’un périphérique mobile en relation avec les antennes de téléphonie mobile transmettant vers ce périphérique.

**Piratage sur internet** – charger (exporter) ou télécharger (importer) sur internet des supports soumis à des droits d’auteur.

**Service de localisation** – service fournissant la localisation d’un périphérique dans le monde hors ligne, qu’il soit mobile ou fixe.

**Logiciel malveillant** – logiciel conçu pour endommager ou désactiver des ordinateurs et des systèmes informatiques. Le logiciel malveillant peut être un logiciel espion, un virus, un cheval de Troie ou un vers informatique.

**Hameçonnage (Phishing)** – Essayer d’obtenir des informations personnelles, comme des noms d’utilisateurs, des mots de passe et des numéros de cartes de crédit, en envoyant un message, que ce soit en ligne ou par téléphone, en se faisant passer pour une organisation légitime.

**Podcast** – Série de fichiers médias numériques, que ce soit audio ou vidéo, qui sont diffusés par épisodes et téléchargés ou écoutés en ligne.

**Code QR** – Un code barre qui peut être lu par les périphériques mobiles, avec une caméra qui redirige l’utilisateur vers un site web lorsqu’il est scanné.

**SKYPE** – programme informatique populaire qui permet aux utilisateurs de créer des profils, de passer des appels téléphoniques gratuitement, de chatter en audio et en vidéo par l’intermédiaire de leur ordinateur ou périphérique mobile à partir de tout point dans le monde.

**Logiciel de sécurité** – Logiciel qui protège un ordinateur d’un certain nombre de menaces.

**Streaming** – Manière d’envoyer des données par un réseau informatique en flux continu et régulier, permettant la diffusion du contenu pendant la réception du reste des données.

**Twitter** – Service de réseau social qui permet à des utilisateurs d’envoyer et de lire de courts messages ou tweets d’autres utilisateurs (140 caractères maximum).

**Tagging (ou marquage)** – Identifier une personne apparaissant sur une photo ou une vidéo en ligne en lui attribuant une étiquette virtuelle avec son nom ou “tag”.

Nous tenons à remercier tout particulièrement Symantec qui apporte son soutien à cette initiative.







World Association  
of Girl Guides  
and Girl Scouts

Association mondiale  
des Guides et des  
Éclaireuses

Asociación  
Mundial de las  
Guías Scouts

#### **FAITES-NOUS PART DE VOS COMMENTAIRES**

Si vous souhaitez écrire à l'éditeur, veuillez envoyer un e-mail à [ourworld@wagggsworld.org](mailto:ourworld@wagggsworld.org) ou nous contacter par courrier à l'adresse suivante : Communications team, World Bureau, Olave Centre, 12c Lyndhurst Road, Londres NW3 5PQ. Il se peut que certaines lettres soient publiées dans de futurs numéros. Les lettres pourront être réduites ou éditées pour plus de clarté.

#### **SOUTENIR NOTRE TRAVAIL DANS LE MONDE ENTIER...**

Aidez-nous à transformer la vie des filles et des jeunes femmes

Donner de l'autonomie aux filles et aux jeunes femmes est la clé du réel changement. Aidez-nous à permettre à des millions de filles et de jeunes femmes de devenir elles-mêmes actrices du changement avec un impact sur leur foyer, leur communauté, leur pays et notre monde.

En soutenant le Fonds mondial pour les filles, vous participez à fournir aux filles et aux jeunes femmes dans le monde des programmes qui les dotent de confiance en soi, compétences en leadership et plaidoyer, ainsi que d'opportunités.

#### **CHANGER SON AVENIR, C'EST CHANGER NOTRE MONDE !**

Faites la promesse de votre soutien aujourd'hui sur [www.theglobalgirlsfund.com](http://www.theglobalgirlsfund.com) ou adressez-nous un email à [enquiries@theglobalgirlsfund.com](mailto:enquiries@theglobalgirlsfund.com) pour découvrir comment vous pouvez vous impliquer.

Association Mondiale des guides et des éclaireuses  
Bureau mondial, Centre Olave  
12c Lyndhurst Road, Londres NW3 5PQ, Angleterre  
téléphone: +44 (0)20 7794 1181  
facsimile: +44 (0)20 7431 3764  
email: [ourworld@wagggsworld.org](mailto:ourworld@wagggsworld.org)  
[www.wagggsworld.org](http://www.wagggsworld.org)

Association caritative enregistrée en Angleterre et au Pays de Galles sous le No 306125