Google

Futé
Vigilant
Secret
Sympa
Courageux

Les Cyber Héros

Dossier pédagogique sur la sécurité en ligne et la citoyenneté numérique

Les
Cyber Héros

Bienvenue dans le dossier pédagogique ‘Les Cyber Héros’ à l’usage des parents, conçu pour accompagner les plus jeunes dans l’apprentissage des connaissances dont ils ont besoin pour explorer le Net en toute sécurité.

Le programme “Les Cyber Héros” fournit aux parents les outils et méthodes nécessaires pour aborder le thème de la sécurité en ligne à la maison. Ce dossier, essentiellement pensé à l’attention des enfants de 8 à 12 ans, propose des méthodes didactiques essentielles. Il offre un cadre de référence aux parents désireux de doter leurs enfants des savoirs et savoir-faire adéquats pour devenir des citoyens numériques prudents et responsables.

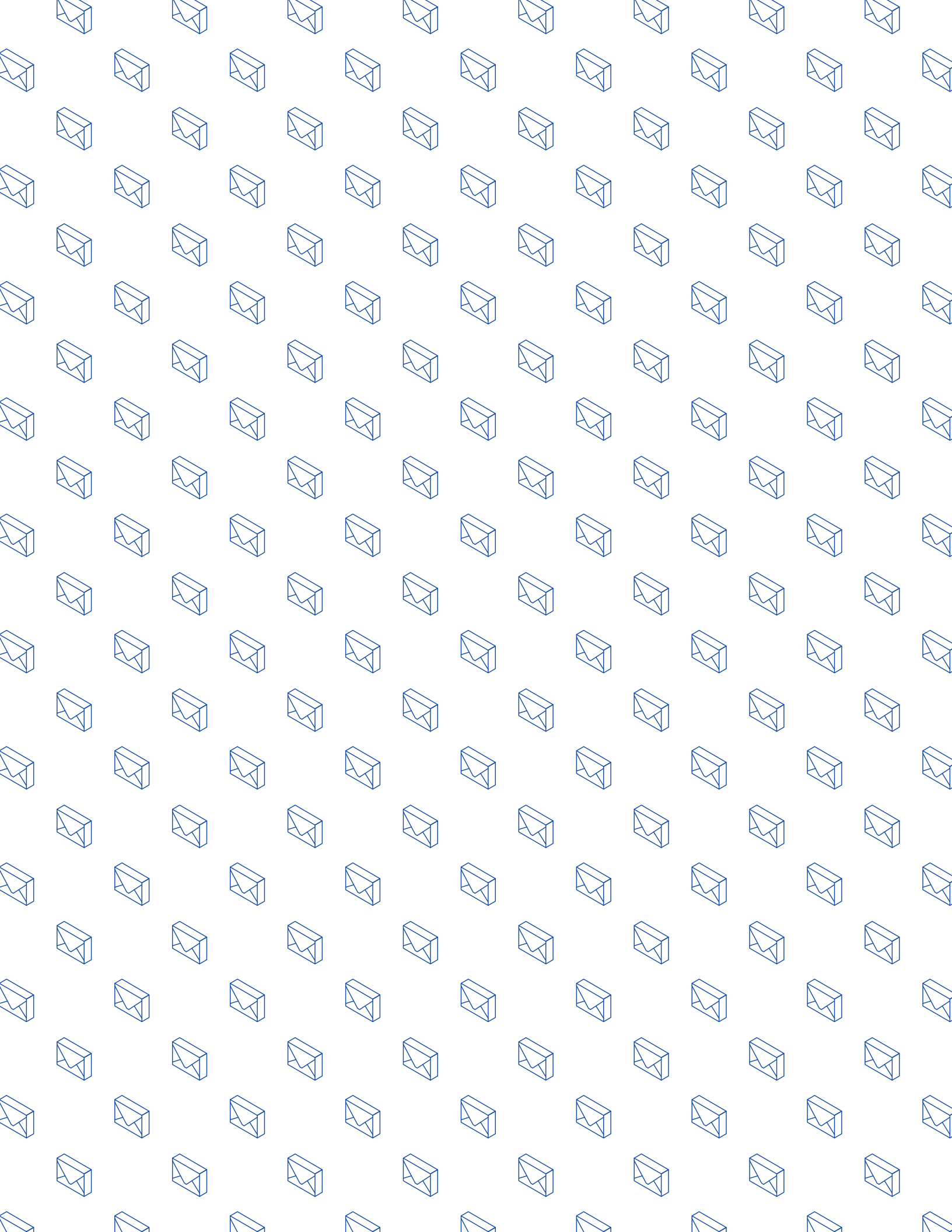
Les cinq piliers de la citoyenneté et de la sécurité numériques sont :

- **Réfléchis bien avant de partager. Sois cyber futé !**
- **Ne tombe pas dans le panneau. Sois cyber vigilant !**
- **Un secret, c’est sacré. Sois cyber secret !**
- **Être gentil, c’est cool. Sois cyber sympa !**
- **En cas de doute, parles-en. Sois cyber courageux !**

Ces thématiques sont également reprises dans Interland, un jeu éducatif dédié à la sécurité en ligne, accessible sur ordinateur depuis n’importe quel navigateur. Qu’il s’agisse d’Interland ou du programme ‘Les Cyber Héros’ dans son ensemble, les parents pourront sélectionner les activités correspondant le mieux aux besoins de leurs enfants, ou suivre l’intégralité du parcours du début à la fin.

Le programme ‘Les Cyber Héros’ est le fruit d’une collaboration étroite entre Test Achats, Bibliothèques Sans Frontières, Child Focus et Google.

Sommaire



Thématique 1 : Sois Cyber futé

Réfléchis bien avant de partager

Se protéger et protéger son image en ligne

Aperçu de la thématique

Activité 1 : **Savoir quand ne pas partager**
Activité 2 : **Protéger les informations confidentielles**
Activité 3 : **Interland : La montagne de la prudence**

Thèmes

Les enseignants et les parents mesurent combien des erreurs commises en ligne par le passé peuvent heurter les sentiments d'une personne, entacher sa réputation et affecter sa vie privée. Il peut être plus difficile de convaincre les enfants qu'un post apparemment inoffensif aujourd'hui puisse être mal compris demain par des personnes dont ils n'avaient jamais imaginé qu'elles le verraient.

Les activités des pages suivantes s'appuient sur des exemples concrets visant à favoriser la discussion et la réflexion, afin que les enfants conservent une image positive en ligne en protégeant leur vie privée et leurs informations personnelles.

Objectifs pour les enfants

- ✓ **Se forger et préserver** une bonne image, en ligne et hors connexion.
- ✓ **Respecter** les limites des autres en matière de vie privée, même si elles diffèrent des nôtres.
- ✓ **Mesurer** les éventuelles répercussions d'une mauvaise gestion de l'empreinte numérique.
- ✓ **Solliciter** l'aide d'un adulte dans les situations délicates.

Réfléchis bien avant de partager
Vocabulaire

Confidentialité en ligne : terme général qui désigne la capacité d'une personne à contrôler quelles informations la concernant sont accessibles, qui peut les voir et qui peut les partager.

Empreinte numérique (ou présence en ligne) : ensemble des informations en ligne qui vous concernent (par exemple, des photos, des contenus audio, des vidéos, du texte, voire même des "J'aime" ou des commentaires que vous avez publiés sur les profils de proches). Tout comme vos pas laissent des empreintes sur le sol, ce que vous publiez en ligne laisse également une trace.

Image en ligne : idées, opinions, impressions ou croyances d'autres personnes à votre sujet. On ne peut jamais être totalement sûr de l'image qu'on a, mais on préfère généralement qu'elle soit bonne !

Informations personnelles : informations se rapportant à une personne spécifique, que ce soit votre nom, votre adresse postale, votre numéro de téléphone, votre numéro de sécurité sociale, votre adresse e-mail, etc. On parle également d'informations "sensibles". Réfléchissez bien avant de partager en ligne ce type d'informations !

Paramètres : section d'une application, d'un produit en ligne, d'un site Web, etc, où vous pouvez définir ou modifier ce que vous partagez et la façon dont votre compte est géré, y compris vos paramètres de confidentialité.

Réfléchis bien avant de partager : Activité 1

Savoir quand ne pas partager

Imaginez des personnages, puis examinez les ensemble pour comprendre la notion de confidentialité.

Objectifs pour les enfants

- ✓ **Comprendre** quels types d'informations doivent rester confidentiels.
- ✓ **Souligner** que chaque personne mérite le respect de ses choix en matière de confidentialité.

Discussion

En quoi la confidentialité est-elle importante ?

Votre empreinte numérique désigne tout ce qui se rapporte à vous en ligne. Il peut s'agir de photos, de contenus audio, de vidéos, de textes, de "Likes" et de commentaires que vous avez laissés sur le profil de vos amis. Que ce soit hors connexion (comme à l'école) ou en ligne, il est tout aussi important d'avoir une empreinte positive.

Avec Internet, il est aujourd'hui très simple de communiquer avec votre famille, vos proches ou d'autres personnes qui ont les mêmes centres d'intérêt que vous. Nous envoyons des messages, partageons des photos et rejoignons des conversations sur les réseaux sociaux, cela sans toujours penser aux autres personnes susceptibles de les voir également. Par exemple, un post (ou une photo) que vous estimez drôle et inoffensif aujourd'hui peut être mal vu et mal interprété par des personnes dont vous n'aviez jamais imaginé qu'elles le verraient, que ce soit aujourd'hui ou bien plus tard. Et une fois qu'un contenu est publié, il est très difficile de l'effacer complètement. N'oubliez pas :

- Comme toute autre chose sur Internet, votre empreinte numérique est visible par des personnes que vous n'avez jamais rencontrées.
- Une fois qu'un contenu vous concernant est en ligne, que vous l'ayez publié ou non, il peut y rester de manière définitive. Pensez-y comme à un texte rédigé au feutre indélébile, que vous ne pourriez jamais effacer même après avoir réalisé que vous vouliez écrire autre chose.

Voilà pourquoi votre confidentialité est importante. La meilleure protection consiste à ne partager que ce dont vous êtes sûr(e). Autrement dit, faites attention à ce que vous publiez et partagez en ligne.

Il est bon de savoir quand ne rien publier du tout, c'est-à-dire ne pas réagir à un post, une photo ou un commentaire de quelqu'un, ni partager un contenu inexact. Si tout le monde s'est déjà entendu dire "Réfléchis bien avant de publier", c'est qu'il s'agit tout simplement d'un très bon conseil. Pour que votre confidentialité et celle des autres soient respectées, il suffit de se demander ce qu'il convient de publier, qui est susceptible de voir votre message, quelles seraient les répercussions pour vous et les autres, et quand ne rien publier du tout.

Voici quelques questions pour prolonger la discussion :

- Quand est-il envisageable de partager une photo ou une vidéo de quelqu'un d'autre ?
- Pourquoi les secrets sont-ils si difficiles à garder ?
- Est-ce qu'il y a des situations dans lesquelles il est acceptable de divulguer le secret de quelqu'un d'autre ?
- Que faire si le post d'une personne qui vous est chère vous laisse penser que celle-ci est en danger ? Si vous estimez que vous devriez partager son secret, devez-vous l'en informer avant de faire quoi que ce soit ? Doit-elle savoir que vous êtes inquiet(e) ?

Activité

1. Proposez à vos enfants d'inventer un personnage de la même tranche d'âge qu'eux et de le dessiner ou d'en écrire le nom au centre d'une feuille de papier. Tout autour, ils dessinent ou écrivent des informations personnelles propre à ce personnage.

2. Examinez chaque information personnelle ensemble, et questionnez à chaque fois s'il est pertinent de la partager en ligne. Quels peuvent être les effets de ce partage sur la réputation en ligne du personnage ?

À retenir

Les informations privées rassemblent des données personnelles ou des faits que nous souhaiterions conserver pour nous-mêmes ou partager seulement avec sa famille ou des amis de confiance. Quel genre d'information cela comprend-il ?

- Votre adresse personnelle et votre numéro de téléphone
- Votre adresse e-mail
- Vos mots de passe
- Vos noms d'utilisateur
- Vos devoirs et les autres documents que vous créez

Réfléchis bien avant de partager : Activité 2

Protéger les informations confidentielles

Les enfants étudient quatre scénarios écrits. Discutez ensuite de la meilleure solution à adopter pour chacun en termes de confidentialité.

Objectifs pour les enfants

- ✓ **Examiner** la question de la confidentialité à partir du point de vue de différentes personnes.
- ✓ **Comprendre** comment différentes situations exigent différents niveaux de confidentialité.

Discussion

Voici quelques scénarios à étudier avec vos enfants :

Scénario 1 : un enfant que vous connaissez s'est fait piquer par un insecte. De vilains boutons sont apparues sur son ventre, et elle ne tient pas à ce que cela se sache.

- Est-ce que les autres ont le droit de savoir ?
- Est-ce à vous de leur dire ?

Scénario 2 : une personne copie le contenu du journal personnel d'une autre et le publie en ligne.

- A-t-elle eu tort de le faire ?
- Que ressentiriez-vous si quelqu'un en faisait autant avec une information que vouliez garder secrète ?

Scénario 3 : une personne souhaite, via un réseau social, de bonnes vacances à un ami sur la page de ce dernier.

- Cet ami avait-il annoncé publiquement qu'il partait ? Est-ce qu'il tient à ce que tout le monde le sache ?
- Y a-t-il d'autres moyens plus confidentiels de communiquer ce message (par exemple, en envoyant un SMS ou un message privé) ?

Scénario 4 : vous savez qu'un camarade de classe a créé un faux compte sur un réseau social afin de se faire passer pour quelqu'un d'autre et de publier des informations personnelles et des messages négatifs à son sujet.

- La victime a-t-elle le droit de savoir ?
- Est-ce que quelqu'un doit le dire à un enseignant ou à un adulte de confiance ? Comment ? Que peut-il se passer si personne ne le fait ?
- Même si le coupable n'est pas identifié clairement, vous savez qui c'est. Devez-vous le dire à un adulte en qui vous avez confiance ?

Activité

Examinez les quatre scénarios avec vos enfants et discutez ensemble de vos conclusions. Notez que chaque scénario peut avoir plusieurs solutions !

À retenir

Que ce soit en ligne ou non, la solution varie selon la situation. Par ailleurs, chacun a le choix en matière de confidentialité et il est important de le respecter, même si vous n'êtes pas toujours tout à fait d'accord.

Réfléchis bien avant de partager : Activité 3

Interland : La montagne de la prudence

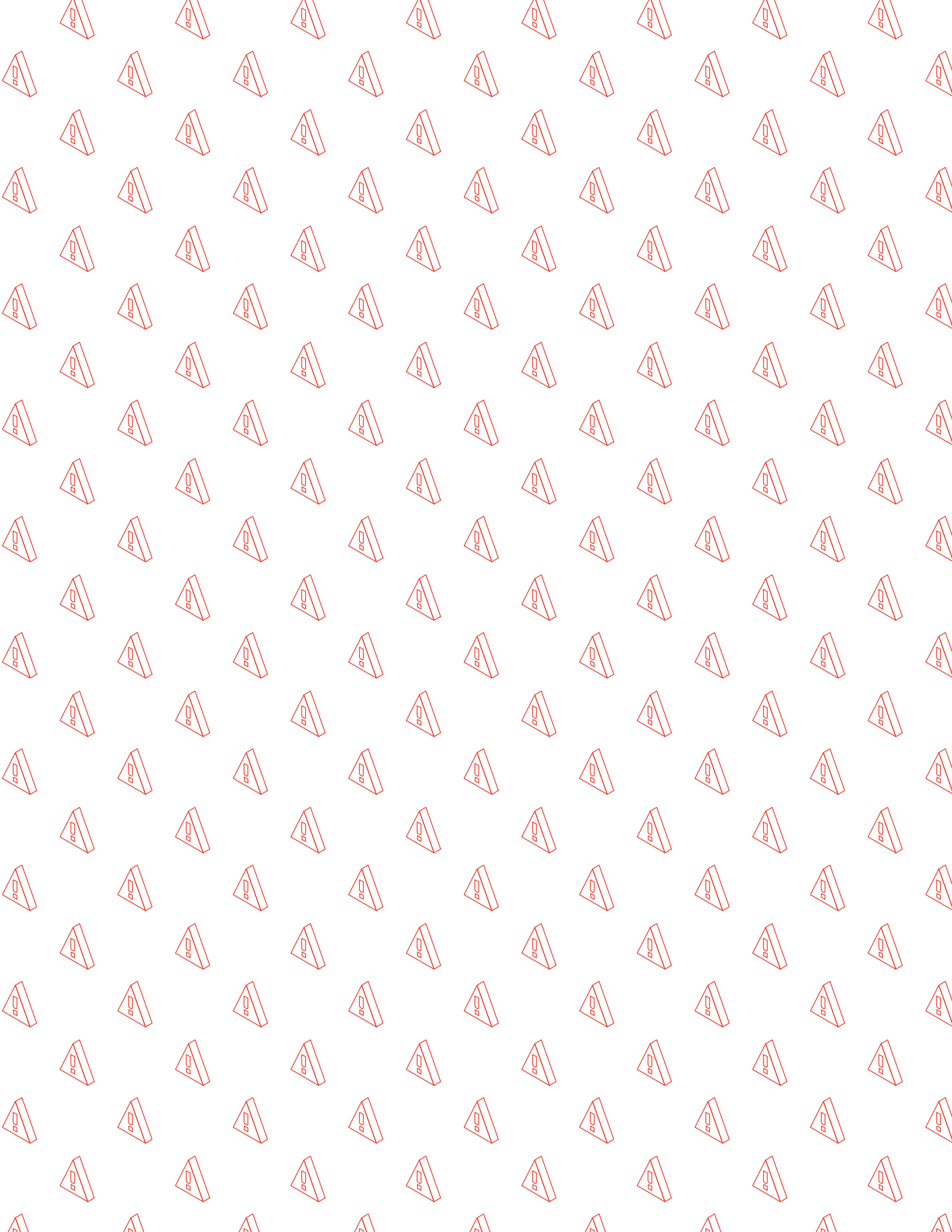
Dans les sommets montagneux d'Interland, la grand-place est un lieu où tout le monde se croise et discute. Mais chacun doit bien réfléchir à ce qu'il peut partager et avec qui... En ligne, les informations se propagent à la vitesse de la lumière et il se trouve qu'un partageur indiscret se cache parmi les internautes.

Depuis votre ordinateur, ouvrez un navigateur Web et rendez vous sur cybersimple.be/interland.
Accédez ensuite à la montagne de la prudence.

Sujets de discussion

Demandez aux enfants de jouer à "La montagne de la prudence" et de répondre aux questions ci-dessous pour discuter plus en détail des enseignements à tirer de ce jeu.

- Parmi tout ce que vous avez publié dans le jeu, quels types de posts partagez-vous le plus souvent dans la vraie vie ? Pourquoi ?
- Décrivez un moment où vous avez malencontreusement partagé une information que vous n'auriez pas dû.
- À votre avis, pourquoi le personnage du jeu "La montagne de la prudence" est-il désigné comme un "partageur indiscret" ?
- Décrivez ce partageur indiscret et dans quelles mesures ses actions affectent le jeu.
- Ce jeu va-t-il changer votre façon de partager des informations avec d'autres personnes en ligne ?
- Citez une chose que vous feriez différemment après avoir suivi ces activités et joué à ce jeu.
- Indiquez une conséquence négative possible liée au fait de partager des informations publiquement au lieu de les limiter à votre cercle d'amis ?
- Que pouvez-vous faire si vous partagez des informations sans faire exprès ? Que faire si une personne vous divulgue par erreur une information très personnelle ?



Thématique 2 : Sois cyber vigilant

Ne tombe pas dans le panneau

Faire attention aux escroqueries et aux tentatives d'hameçonnage

Aperçu de la thématique

Activité 1 : **Ne pas mordre à l'hameçon !**
Activité 2 : **Mais qui est-ce exactement ?**
Activité 3 : **À propos des "bots"**
Activité 4 : **Interland : La rivière de la réalité**

Thèmes

Les enfants doivent comprendre que les informations qu'ils trouvent en ligne ne sont pas nécessairement vraies ou fiables, et que certains esprits malveillants cherchent avant tout à leur soutirer des informations ou à usurper leur identité. L'hameçonnage et les escroqueries en ligne amènent les internautes de tous âges à réagir aux propositions de personnes qu'ils ne connaissent pas ou qui se font parfois passer pour des proches.

Objectifs pour les enfants

- ✓ **Comprendre** que ce qui figure en ligne n'est pas nécessairement vrai.
- ✓ **Apprendre** comment fonctionne l'hameçonnage, en quoi il constitue une menace et les solutions pour l'éviter.
- ✓ **Déterminer** la validité des sites Web et des sources d'information, et se méfier des manipulations, des demandes non fondées, des fausses offres, des prix mensongers et autres escroqueries en ligne.

Ne tombe pas dans le panneau
Vocabulaire

Bot (ou “chatbot” ou assistant virtuel”) : également appelé “chatbot” ou “assistant virtuel”, ce type de logiciel qui fonctionne en ligne ou sur un réseau, est chargé de répondre automatiquement à des questions, de suivre des commandes (comme donner l’itinéraire pour aller chez un nouvel ami) ou d’effectuer des tâches simples (comme diffuser un titre musical).

Hameçonnage : technique dont le but est de vous escroquer ou de vous inciter à partager des informations de connexion ou toute autre donnée personnelle en ligne, que ce soit par e-mail, dans des annonces ou sur des sites qui ressemblent à ceux auxquels vous êtes habitués.

Harponnage : escroquerie par hameçonnage où le pirate utilise des éléments de vos informations personnelles pour vous cibler spécifiquement.

Escroquerie : tentative malhonnête de gagner de l’argent ou quelque chose de valeur en trompant les gens.

Fiable : auquel on peut se fier pour effectuer ce qui est juste ou nécessaire.

Authentique : réel, véritable, vrai ou exact (pas faux ni copié).

Vérifiable : dont la véracité ou l’exactitude peut être prouvée ou démontrée.

Trompeur : faux, mensonger ou action ou message qui vise à duper ou induire en erreur une personne.

Manipulation : action qui vise à contrôler ou à influencer une personne ou une situation de manière abusive, malhonnête ou sous la menace ou d’un élément trafiqué disponible en ligne, tel qu’une photo qui a été retouchée pour vous faire croire qu’une chose fausse est vraie.

Frauduleux : qui vise à duper une personne pour lui soutirer une chose présentant une valeur.

Pare-feu : programme qui protège votre ordinateur de la plupart des escroqueries.

Malveillant : action ou mot visant à être blessant ou cruel. Peut également se rapporter à des logiciels dont le but est d’endommager l’appareil, le compte ou les informations personnelles de quelqu’un.

Catfishing : technique qui consiste à créer une fausse identité ou un faux compte sur un réseau social pour inciter les gens à partager leurs informations personnelles en croyant qu’ils s’adressent à une vraie personne ou à une page légitime.

Piège à clics (ou “clickbait”) : méthode consistant à inciter les internautes à cliquer sur un lien en utilisant un texte ou une image qui stimule la curiosité, souvent de façon trompeuse. Ce type de technique peut viser à transmettre un virus ou à exposer l’utilisateur à des publicités (afin de réaliser des profits).

Ne tombe pas dans le panneau : Activité 1

Ne pas mordre à l'hameçon!

Dans le cadre d'un jeu, les enfants doivent déterminer parmi différents e-mails et SMS lesquels sont légitimes et lesquels sont des escroqueries par "hameçonnage".

Objectifs pour les enfants

- ✓ **Identifier** les techniques d'usurpation d'identité.
- ✓ **Examiner** les solutions.
- ✓ **Savoir** qu'on peut s'adresser à un adulte de confiance lorsqu'on pense être victime d'une tentative d'usurpation d'identité.
- ✓ **Reconnaître** les signes de tentatives d'hameçonnage.
- ✓ **Faire attention** à la façon de partager ses informations personnelles et avec qui.

Discussion

En quoi consiste l'hameçonnage exactement ?

L'hameçonnage désigne une technique qu'emploie une personne via e-mail, SMS ou toute autre communication en ligne pour vous soutirer des renseignements (par exemple des informations de connexion ou relatives à votre compte) en se faisant passer pour quelqu'un en qui vous avez confiance. L'hameçonnage par e-mail (ainsi que les sites dangereux vers lesquels cette personne essaie de vous orienter ou les pièces jointes qu'elle vous incite à ouvrir) risque également d'exposer votre ordinateur à des virus. Certains virus utilisent votre liste de contacts pour cibler votre famille et vos proches, en procédant de la même façon qu'avec vous ou de manière plus personnalisée. D'autres types d'escroqueries peuvent également prétendre que votre appareil rencontre un problème en vue de vous inciter à télécharger des logiciels malveillants ou indésirables. Gardez toujours à l'esprit qu'un site Web ou une annonce publicitaire n'ont aucun moyen de détecter s'il y a un problème sur votre ordinateur !

Certaines attaques par hameçonnage sont plus faciles à identifier que d'autres, plus sournoises et vraiment convaincantes : par exemple, lorsqu'un escroc vous envoie un message contenant certaines de vos informations personnelles. C'est ce qu'on appelle le "harponnage", qui est parfois très difficile à repérer du fait que la mention de vos informations personnelles dans le message laisse entendre que l'expéditeur vous connaît.

Avant de cliquer sur un lien ou de saisir votre mot de passe sur un site que vous ne connaissez pas, interrogez vous toujours sur la page Web ou le message concerné. Voici quelques questions à vous poser :

- Le site a-t-il l'air professionnel, comme ceux que vous connaissez ou auxquels vous vous fiez, avec par exemple le logo habituel du produit ou de l'entreprise, sans aucune faute d'orthographe ?

- Est-ce que l'URL du site correspond au nom et aux informations du produit ou de l'entreprise que vous recherchez, ou contient-elle des fautes d'orthographe ?
- Y a-t-il des pop-up contenant du spam ?
- Est-ce que l'URL commence par "https://" avec un petit cadenas fermé à gauche ? (cela signifie que la connexion est sécurisée)
- Que contient le texte en petits caractères ? (c'est souvent là que figurent des éléments révélateurs de la tentative d'escroquerie)
- Est-ce que le message ou le site offre quelque chose de trop beau pour être vrai, comme l'opportunité de gagner une grosse somme d'argent ? (c'est presque toujours *trop* beau pour être vrai !)
- Le message vous semble-t-il un peu bizarre ? (comme si l'expéditeur vous connaissait, mais vous n'êtes pas complètement sûrs)

Et que faire si vous tombez dans le panneau ? D'abord, ne paniquez pas !
- Modifiez les mots de passe de vos comptes en ligne.
- Informez aussitôt vos proches et vos contacts, car ils risquent d'être les prochaines cibles.
- Si possible, signalez le message comme du spam (à partir des paramètres).
- Signalez la tentative de hameçonnage auprès du Centre pour la Cyber Sécurité en écrivant à l'adresse suspect@safeonweb.be.

S'ils suspectent une escroquerie, vos enfants doivent avoir en tête d'avertir immédiatement un parent, un enseignant ou un adulte en qui ils ont confiance. Indiquez leur que plus ils attendront, plus la situation risquerait de s'aggraver.

Activité

Matériel nécessaire :

- Fiche d'exercice *Exemples d'hameçonnage*

1. Regardez les exemples

Regardez avec vos enfants les différents exemples de messages et de sites Web fournis.

2. Indiquez vos choix individuellement

Pour chaque exemple, indiquez si le message ou le site est sérieux ou s'il s'agit d'une escroquerie. Énumérez vos raisons en dessous.

3. Discutez de vos choix

Quels exemples semblaient fiables et quels autres étaient suspects ?
Y a-t-il des réponses qui vous ont surpris ? Si oui, en quoi ?

4. Continuez la discussion

Voici d'autres questions à vous poser au sujet de messages et de sites que vous trouvez en ligne :

- **Ce message a-t-il l'air fiable ?**
  Quelle est votre première impression ? Avez-vous remarqué des éléments suspects ? Est-ce que l'on vous propose de résoudre un soi-disant problème ?

Réponses pour chaque exemple présenté dans la fiche d'exercice :

1. **Fiable.** L'utilisateur est invité par e-mail à se rendre sur le site Web du cinéma pour se connecter lui-même à son compte, plutôt que par l'intermédiaire d'un lien susceptible de le diriger vers un site Web malveillant, et sans avoir à envoyer son mot de passe par e-mail.
2. **Escroquerie.** URL suspecte et non sécurisée.
3. **Fiable.** URL sécurisée qui commence par https:// et précédée par le petit cadenas vert.
4. **Escroquerie.** Offre suspecte en échange de coordonnées bancaires.
5. **Escroquerie.** URL suspecte et non sécurisée.

- **Vous propose-t-on quelque chose de gratuit ?**
  Les offres gratuites ne sont généralement pas vraiment gratuites.
- **Est-ce que l'on vous demande des informations personnelles ?**
  Certains sites Web vous demandent des informations afin de vous envoyer encore plus de messages destinés à vous escroquer (par exemple, des questionnaires ou des "tests de personnalité" visant à rassembler des informations sur vous afin de deviner plus facilement votre mot de passe ou d'autres données confidentielles). La plupart des vraies entreprises ne vous demandent pas d'informations personnelles par e-mail.
- **Est-ce une chaîne d'e-mails ou un post sur un réseau social ?**
  Les e-mails et les posts que vous êtes invités à transmettre à toutes vos connaissances peuvent présenter des risques pour vous comme pour les autres. Ne le faites pas sauf si vous êtes convaincus de la fiabilité de l'expéditeur ou du message.
- **Y a-t-il du texte en petits caractères ?**
  En bas de la plupart des documents, vous pouvez trouver ce que l'on appelle les "petits caractères". Il s'agit d'un texte succinct contenant souvent des informations faites pour que vous n'y prêtiez pas attention. Par exemple, le titre en haut d'un message peut indiquer que vous avez gagné un téléphone, alors que les petits caractères préciseront que vous devez en fait payer 200€ par mois. Alors faites y attention : ces petites lignes ont leur importance.

Remarque : pour les besoins de cet exercice, partez du principe que la messagerie "Internaut" est fiable.

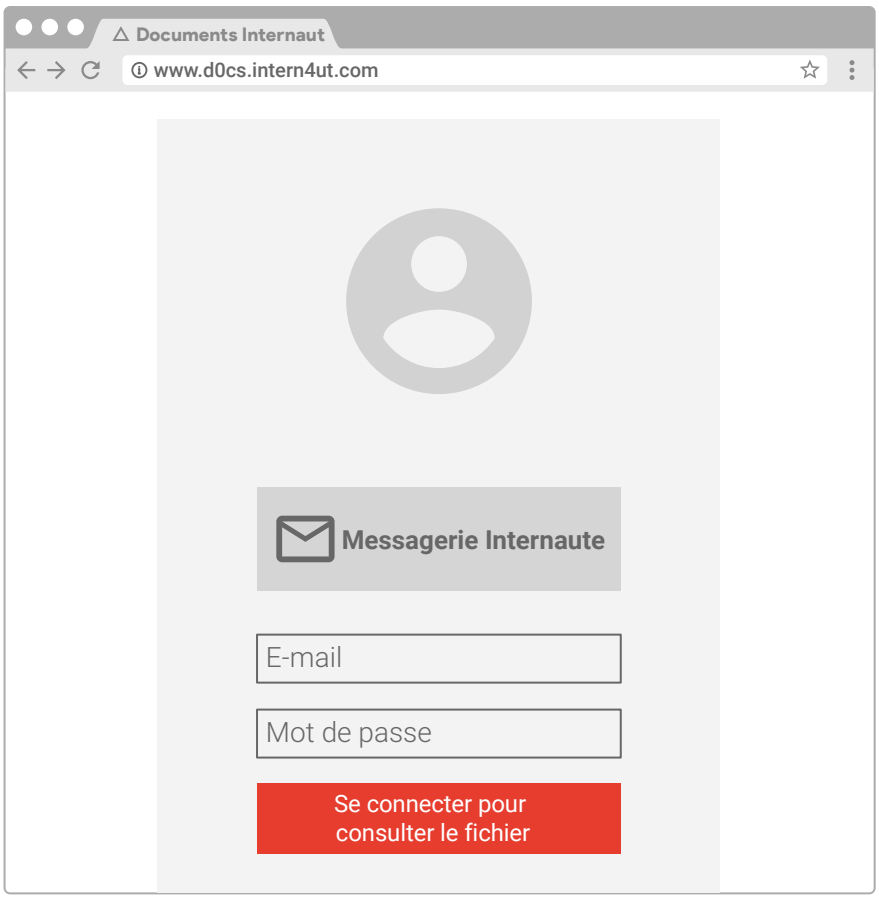
À retenir

Lorsque vous êtes en ligne, faites toujours attention aux tentatives d'hameçonnage par e-mail, par message instantané ou dans les posts. Et si vous vous faites berner, avertissez immédiatement un adulte en qui vous avez confiance.

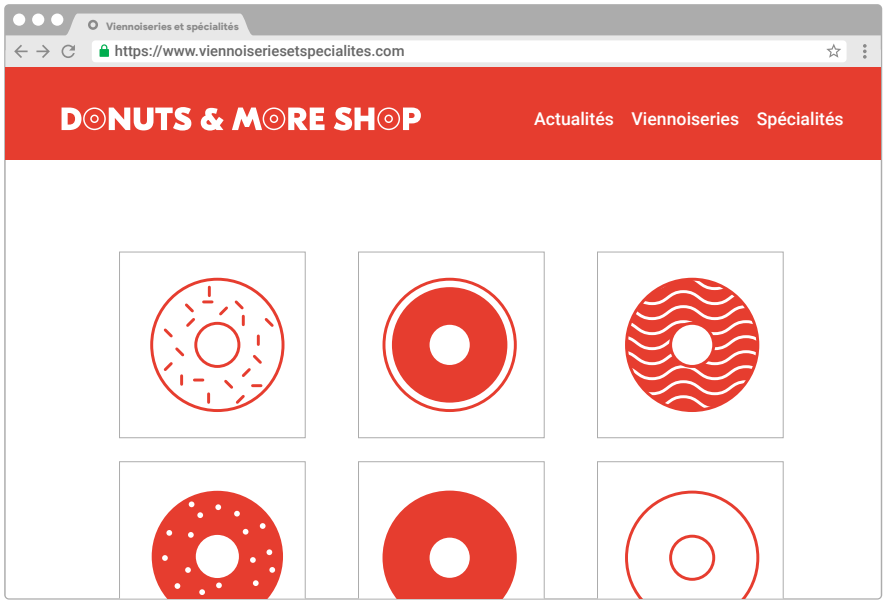
Fiche d’exercice – Activité 1

Exemples d’hameçonnage

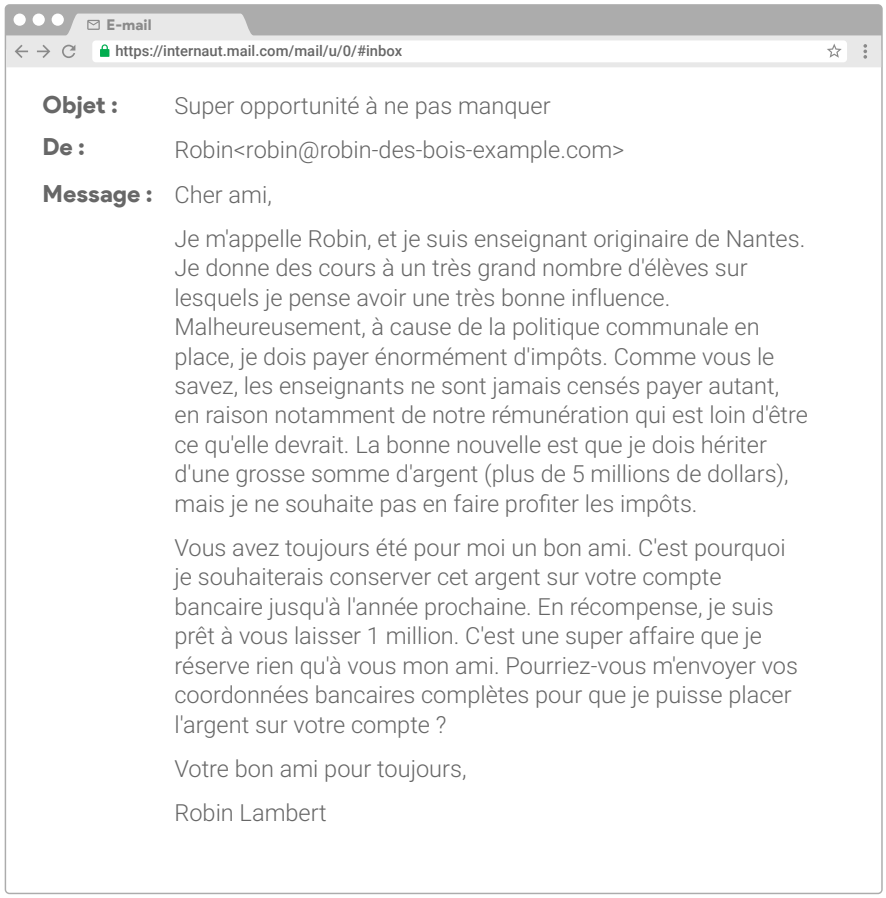
1. Ce message est-il fiable ou est-ce un cas de hameçonnage ?



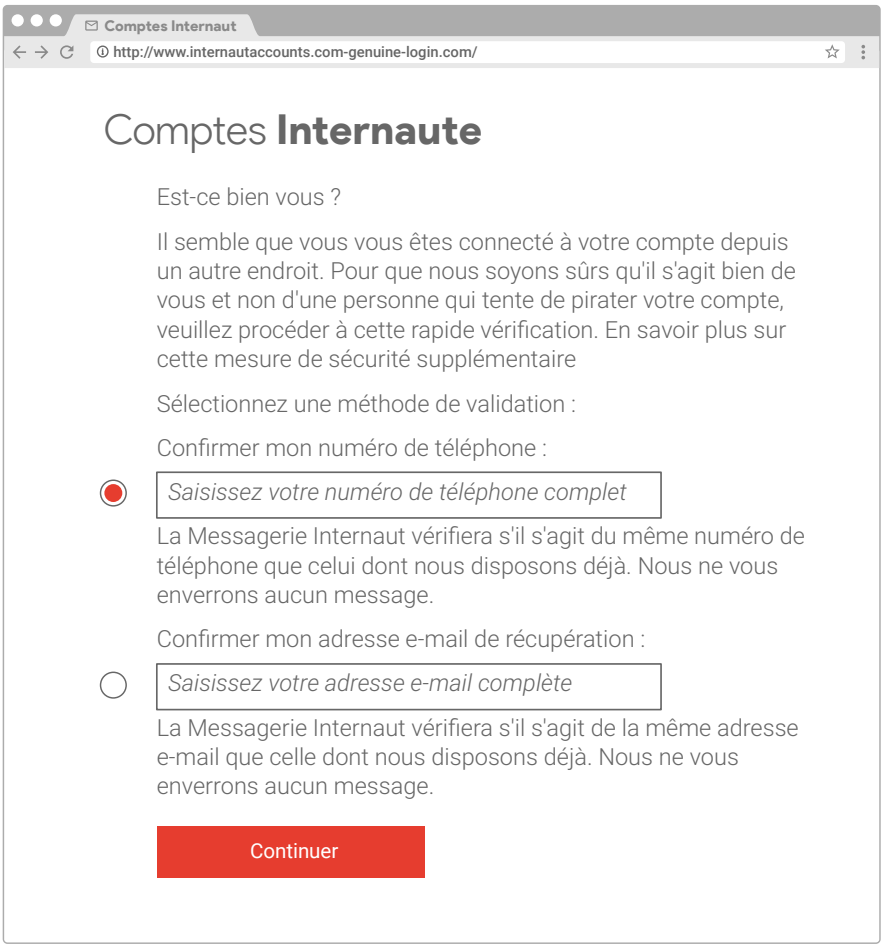
2. Cette page est-elle fiable, ou est-ce un cas de hameçonnage ?



3. Ce site est-il fiable ou s'agit-il d'une escroquerie ?



4. Ce message est-il fiable, ou est-ce du hameçonnage ?



5. Ce message est-il fiable, ou est-ce du hameçonnage ?

Ne tombe pas dans le panneau : Activité 2

Mais qui est-ce exactement ?

Les enfants mettent en pratique les connaissances acquises lors de l'activité précédente. Ils reproduisent différents scénarios et discutent des réponses possibles contre les tentatives d'hameçonnage que ce soit par e-mail, dans des posts, des images ou n'importe quel texte en ligne.

Objectifs pour les enfants

- ✓ **Comprendre** qu'une personne en ligne peut ne pas être celle qu'elle prétend.
- ✓ **S'assurer** que cette personne est bien celle qu'elle prétend avant de lui répondre.
- ✓ **Poser des questions** ou solliciter l'aide d'un adulte s'il est difficile de déterminer qui est cette personne.

Discussion

Comment savoir si une personne est bien celle qu'elle prétend ?

Lorsque vous êtes au téléphone avec un ami, vous savez que c'est lui au son de sa voix, même si vous ne le voyez pas. Mais lorsque vous êtes en ligne, c'est quelque peu différent. En effet, il est parfois compliqué d'être sûr qu'une personne est bien celle qu'elle prétend. Par exemple, dans les applications et les jeux, des utilisateurs se font parfois passer pour d'autres pour plaisanter ou mettre la pagaille. Dans d'autres cas, certains usurpent l'identité d'autres pour voler des informations personnelles.

De même, des internautes que vous ne connaissez pas peuvent vous demander d'entrer en contact. La solution la plus sûre est de ne pas répondre ou d'avertir un parent ou un adulte de confiance. En revanche, si vous décidez de répondre favorablement, commencez par vous renseigner sur lui. Consultez son profil, regardez qui sont ses amis, ou recherchez des informations qui confirment qu'il est bien celui qu'il prétend être.

Il y a de nombreux moyens de vérifier l'identité d'une personne en ligne. En voici quelques exemples pour commencer.

- **La photo de profil de la personne est-elle suspecte ?**
  Est-elle floue ou le visage est-il difficile à discerner ? Est-ce un avatar ou un personnage de dessin animé à la place ? Ou n'y a-t-il carrément aucune photo ? Sur les réseaux sociaux, il est très facile de dissimuler son identité avec des photos de mauvaise qualité, des avatars, des photos d'animaux, etc. Certains fraudeurs vont même jusqu'à voler la photo d'une vraie personne pour créer un faux profil et se faire passer pour elle. Pouvez-vous trouver d'autres photos de la personne avec le même nom associé ?

- **Le nom d'utilisateur contient-il le vrai nom de la personne ?**
  Sur les réseaux sociaux, est-ce que cette personne utilise son vrai nom comme pseudonyme ?

- **Le profil de la personne inclut-il une biographie sur elle ?**
  Si tel est le cas, a-t-elle l'air d'avoir été rédigée par une vraie personne ? Les faux comptes ne fournissent pas beaucoup de renseignements sur la personne ou contiennent alors tout un tas d'informations rassemblées au hasard pour créer un faux profil. La biographie indique-t-elle quoi que ce soit que vous pouvez vérifier en effectuant une recherche ?

- **Depuis combien de temps le compte est-il actif ? Les activités affichées correspondent-elles à ce que vous pensiez ?**
  Est-ce un nouveau profil ou y a-t-il beaucoup d'activités dessus ? Avez-vous des amis en commun avec cette personne comme vous le pensiez ? De manière générale, les faux comptes ne contiennent pas beaucoup de posts, de commentaires ou d'échanges avec d'autres personnes.

Activité

Matériel nécessaire :

- Un exemplaire de la fiche d'exercice *Mais qui est-ce exactement ?*, que vous aurez découpée en bandes et où figure un scénario sur chaque bande.
- Un bol dans lequel mettre toutes les bandes de papier.

Étudiez un ou plusieurs scénarios et expliquez l'un après l'autre comment, selon vous, vous devriez réagir à cette situation. Si vous êtes trois ou plus, vous pouvez commencer en jouant un scénario (une personne raconte, une seconde exprime le message par des gestes, une troisième répond, une quatrième explique le raisonnement...), puis discutez-en tout en vérifiant la feuille. N'hésitez pas à imaginer d'autres messages qui, selon vous, auraient été encore plus délicats à traiter.

À retenir

C'est vous qui décidez à qui vous parlez en ligne. Assurez-vous que les personnes avec qui vous échangez sont bien celles qu'elles prétendent être !

Fiche d'exercice : Activité 2

Mais qui est-ce exactement ?

Voici cinq scénarios s'inspirant de messages que n'importe qui peut recevoir en ligne ou sur son téléphone. Différentes solutions sont proposées pour chacun : certaines bonnes, d'autres moins. Regardez lesquelles vous paraissent censées ou si d'autres solutions vous viennent à l'esprit. Si vous rencontrez une de ces situations sans savoir vraiment quoi faire, la solution la plus simple est de ne pas répondre. Vous pouvez également les ignorer ou les bloquer. Et il est même conseillé d'en parler à un parent ou à un enseignant.

Scénario 1

Vous recevez ce message d'une personne que vous ne reconnaissez pas : "Salut ! Tu as l'air sympa, et j'aimerais bien faire ta connaissance. Tu vas voir, on va bien s'amuser ! Peux-tu m'ajouter à ta liste d'amis ? Rémi" Que devez-vous faire ?

- **Ignorer Rémi.** Si vous ne le connaissez pas, vous pouvez tout simplement décider de ne pas lui parler, un point c'est tout.
- **Répondre : "Bonjour Rémi. Est-ce que je te connais ?"** En cas de doute, contactez-le d'abord.
- **Bloquer Rémi.** Si vous avez décidé de le bloquer après avoir vérifié qui il est, vous ne recevrez plus de messages de lui. Sur la plupart des plates-formes de réseaux sociaux, il ne saura même pas que vous l'avez bloqué.
- **Consulter le profil de Rémi.** Faites attention aux faux profils qui sont faciles à créer. Regardez sa liste d'amis pour voir avec qui il est en relation. Son cercle d'amis peut également vous montrer si Rémi est une vraie personne ou pas, notamment si vous ne connaissez aucun de ses contacts. Et si rien ne vous a vraiment convaincu sur sa page, cela suppose là aussi que Rémi n'est pas une vraie personne.
- **Ajouter Rémi à votre liste d'amis.** Ajoutez-le uniquement si vous estimez qu'il est fiable. Pour cela, vous devez impérativement avoir vérifié qui il est et averti un adulte en qui vous avez confiance.
- **Donner à Rémi des informations personnelles.** Ne communiquez jamais d'informations personnelles aux personnes que vous ne connaissez pas.

Scénario 2

Vous recevez un SMS d'une personne dont vous ne vous souvenez pas. "Salut, c'est Tom ! Tu te souviens de moi l'été dernier ?" Que devez-vous faire ?

- **Bloquer Tom.** Ce serait impoli si vous le connaissez vraiment. Cependant, si vous êtes sûrs de n'avoir rencontré personne qui s'appelle Tom l'été dernier, ou s'il vous envoie trop de SMS ou d'informations sur lui, il est alors préférable de le bloquer.
- **Ignorer Tom.** Si vous ne le connaissez pas, vous pouvez tout simplement ne pas lui répondre.

- **Répondre : "Bonjour Tom. Est-ce que je te connais ?"** C'est une bonne solution si vous n'êtes pas sûrs de l'avoir rencontré et si vous voulez vérifier que c'est bien le cas en faisant quelques recherches, mais ne lui dites pas où vous étiez l'été dernier !
- **Répondre : "Je ne me souviens pas de toi, mais on peut quand même se voir un de ces jours."** Ce n'est pas vraiment une bonne idée. Vous ne devez jamais proposer à une personne de la rencontrer si vous ne la connaissez pas.

Scénario 3

Vous recevez un message privé de @fandefoot12 alors que vous ne suivez pas cette personne. "Salut ! J'adore tes posts, t'es super drôle ! Donne-moi ton numéro de GSM pour qu'on discute !" Que devez-vous faire ?

- **Ignorer @fandefoot12.** Vous n'avez pas besoin de répondre si vous n'en avez pas envie.
- **Bloquer @fandefoot12.** Si vous bloquez cette personne, car vous la trouvez bizarre, vous n'entendrez plus jamais parler d'elle, sauf si elle vous contacte avec un faux profil sous un autre nom.
- **Répondre : "Bonjour, est-ce que je te connais ?"** En cas de doute, veillez à poser des questions avant de divulguer des informations personnelles comme votre numéro de téléphone.
- **Répondre : "OK, mon numéro est le…"** Non ! Même si vous avez vérifié l'identité de cette personne, ne communiquez pas d'informations personnelles sur les réseaux sociaux. Trouvez un autre moyen de prendre contact, que ce soit par l'intermédiaire d'un parent, d'un enseignant ou de toute autre personne de confiance.

Scénario 4

Vous recevez un message de chat d'une personne que vous ne connaissez pas. "Je t'ai vu dans le couloir aujourd'hui. T MIGNON ! C'est quoi ton adresse ? Je peux passer." Que devez-vous faire ?

- **Ignorer cette personne.** C'est probablement la bonne solution.
- **Bloquer cette personne.** N'hésitez pas à le faire si vous avez un mauvais pressentiment au sujet de quelqu'un.
- **Répondre : "Qui es-tu ?"** Ce n'est sans doute pas une bonne idée. Si le message semble suspect, mieux vaut peut-être ne pas y répondre ou tout simplement bloquer la personne.
- **Répondre : "C'est toi Laure ? T mignonne toi aussi ! J'habite au 240 boulevard Joffre."**
  Ce n'est pas une bonne idée même si vous pensez savoir de qui il s'agit. Avant de donner votre adresse ou toute autre information personnelle à une personne, vérifiez son identité, même si vous pensez la connaître. Ne rencontrez jamais quelqu'un en personne si vous ne le connaissez qu'à travers vos discussions en ligne.

Scénario 5

Vous recevez le message “Hé, je viens de rencontrer ton amie Sophie ! Elle m’a parlé de toi, je voudrais te rencontrer. Tu habites où ?” Que devez-vous faire ?

- **Ignorer cette personne.** Si vous ne la connaissez pas, mais que vous avez bien une amie qui s’appelle Sophie, la meilleure solution est de contacter cette dernière avant de répondre à ce message.
- **Bloquer cette personne.** Si vous ne connaissez pas l’expéditeur du message et que vous n’avez pas d’amie qui s’appelle Sophie, il est probablement préférable d’accéder aux paramètres afin de le bloquer pour l’empêcher de vous recontacter.
- **Répondre : “Qui es-tu ?”** Ce n’est sans doute pas une très bonne idée. Si vous ne connaissez pas cette personne, il est préférable de ne pas lui répondre, au moins jusqu’à ce que vous revoyiez Sophie pour lui en parler.

Ne tombe pas dans le panneau : Activité 3

À propos des “bots”

Aujourd’hui, les enfants interagissent avec de plus en plus de “voix” non humaines provenant d’appareils, d’applications et de sites, principalement chez eux et peut-être même encore plus à l’école. Ces voix sont parfois appelées “chatbots”, “assistants virtuels” ou tout simplement “bots”. Cette activité simple sous forme de questions/réponses a pour but d’encourager les enfants à discuter ensemble de l’interaction avec ces bots.

Remarque : Assurez-vous que le débat reste ouvert. Cette activité vise à développer l’esprit critique des enfants, plutôt qu’à tirer des conclusions.

Objectifs pour les enfants

- ✓ **Identifier** les technologies interactives de plus en plus présentes dans la vie des enfants.
- ✓ **Examiner** les expériences vécues avec des bots de différentes sortes.
- ✓ **Analyser** l’impact à la fois positif et négatif que ces technologies peuvent avoir au quotidien.

Discussion

Quelques éléments d’explication pour vos enfants :

De plus en plus de gens utilisent aujourd’hui ce que l’on appelle des “bots”. En avez-vous déjà entendu parler ? On les désigne aussi parfois par les termes “chatbots” ou “assistants virtuels”. Ils sont utilisés dans des situations diverses et variées, que ce soit pour jouer, consulter la météo, répondre à des questions, obtenir un itinéraire, être averti lorsque le temps imparti est écoulé, etc. Ces bots ont parfois un nom humain ou qui décrit leur fonction (par exemple, le bot “Teste ton code” permet de réviser le code de la route). Ils peuvent être disponibles en ligne, sur des appareils mobiles ou en voiture. Il peut s’agir également d’appareils spéciaux que les utilisateurs gardent chez eux dans différentes pièces. Voyons ensemble si vous en avez déjà utilisés, et intéressons-nous à leur évolution.

Voici plusieurs questions sur lesquelles nous allons nous pencher :

- Savez-vous ce qu’est un bot ?
- Qui parmi vous a déjà discuté avec un bot ? Sur quel type d’appareil ?
- Qui veut nous raconter son expérience ?
- Selon vous, pour quelle(s) action(s) les bots sont-ils les plus performants (exemples à proposer : pour jouer, donner la météo, les actualités, des informations) ?
- Les bots utilisent ce que l’on appelle l’intelligence artificielle ou IA, qui se nourrit de ce que vous lui demandez afin de vous être encore plus utile par la suite. Pour cela, les bots “mémorisent” ou enregistrent parfois vos questions et vos propos. Avez-vous une idée de ce que vous diriez à un bot ? Si oui, précisez ce que vous lui diriez et indiquez le type d’informations que vous garderiez pour vous.

- Selon vous, est-ce comme si vous parliez à un être humain ? Quelles sont les similitudes et les différences ?
- Comment les personnes que vous connaissez considèrent-elles les bots ou discutent- elles avec ?
- Comment vous adresseriez-vous à un bot ? Seriez-vous gentil ou est-ce que vous crieriez parfois dessus ?
- Les gens peuvent-ils crier sur les bots ? Justifiez votre réponse. (Cela revient-il à pratiquer un certain type d'interaction ?)
- Parfois, les enfants les plus jeunes pensent que les bots sont humains. Que diriez- vous à votre petit frère, à votre petite sœur ou à un petit cousin pour lui faire comprendre avec qui il discute ?
- Si les bots peuvent apprendre de nous, humains, pensez à quelque chose que vous ne voudriez pas que votre bot apprenne ? (Conseil : repensez aux activités de la thématique "Réfléchis bien avant de partager" et discutez-en par rapport aux bots.)

Activité

Au terme de la discussion et à l'aide des appareils à disposition, recherchez des photos de bots et des informations à ce sujet (comme des articles de presse) en saisissant, par exemple, les termes "bots", "chatbots", "assistants virtuels" ou "assistants numériques". Déterminez ensemble avec vos enfants si les informations recueillies sont pertinentes.

À retenir

L'esprit critique est l'un des "outils" les plus efficaces et durables dont nous disposons pour une bonne utilisation des technologies. Et nous l'aiguisons à chaque fois que nous nous en servons, ce qui est une excellente chose. En outre, le fait d'exprimer nos pensées ensemble est un moyen ludique et constructif d'utiliser et d'améliorer cet outil.

Ne tombe pas dans le panneau : Activité 4

Interland : La rivière de la réalité

La rivière qui traverse Interland charrie de vraies et de fausses informations, mais les apparences sont parfois trompeuses. Pour traverser les rapides, utilisez votre bon sens et ne vous laissez pas prendre au petit jeu de l'hameçonneur qui se cache dans les eaux troubles.

Depuis votre ordinateur, ouvrez un navigateur Web et rendez vous sur cybersimple.be/interland.
Accédez ensuite à la rivière de la réalité.

Sujets de discussion

Demandez aux enfants de jouer à "La rivière de la réalité" et de répondre aux questions ci-dessous pour discuter ensuite plus en détail des enseignements à en tirer.

- Décrivez une situation où vous avez dû déterminer si un contenu en ligne était vrai ou faux. Quels signes particuliers avez-vous remarqués ?
- Qu'est-ce qu'un hameçonneur ? Décrivez son comportement et la façon dont il affecte le jeu.
- Ce jeu va-t-il changer votre façon d'évaluer les contenus ou les personnes en ligne ? Si oui, comment ?
- Citez une chose que vous feriez différemment après avoir suivi ces thématiques et joué à ce jeu.
- Quels indices peuvent révéler quelque chose de suspect dans une certaine situation en ligne ?
- Que ressentez-vous lorsque vous êtes face à un contenu douteux en ligne ?
- Si vous n'êtes pas certains du sérieux ou de la véracité d'un contenu, que devez-vous faire ?

Thématique 3 : Sois cyber secret

Un secret, c'est sacré

Mesurer l'importance de la confidentialité et de la sécurité

Aperçu de la thématique

Activité 1 : **Créer un mot de passe sécurisé**
Activité 2 : **Garder son mot de passe secret**
Activité 3 : **Interland : La tour des trésors**

Thèmes

Les problèmes de confidentialité et de sécurité en ligne n'ont pas toujours de solution évidente. Pour protéger vos informations personnelles et confidentielles, autrement dit tout ce qui vous caractérise, vous devez vous poser les bonnes questions et trouver vos propres réponses de manière réfléchie.

Objectifs pour les enfants

- ✓ **Découvrir** en quoi la confidentialité est importante et liée à la sécurité en ligne.
- ✓ **S'exercer** à créer des mots de passe sécurisés.
- ✓ **Passer en revue** les outils et les paramètres de protection contre les pirates informatiques et les autres menaces.

Un secret, c’est sacré
Vocabulaire

Confidentialité : fait de protéger les informations personnelles des utilisateurs (appelées également “informations sensibles”).

Sécurité : fait de protéger les appareils des utilisateurs et les logiciels qui y sont installés.

Validation en deux étapes (appelée également “authentification à deux facteurs” ou “authentification en deux étapes”) : processus de sécurité où la connexion à un service nécessite deux étapes ou “facteurs” distincts, comme un mot de passe et un code à usage unique. Par exemple, vous devrez d’abord saisir votre mot de passe, puis un code qui vous est envoyé par SMS sur votre téléphone ou provenant d’une application.

Mot de passe ou code secret : combinaison secrète pour accéder à quelque chose. Elle peut prendre différentes formes : par exemple, vous devrez saisir un code à quatre chiffres pour verrouiller votre téléphone et un mot de passe plus complexe pour votre compte de messagerie. En général, vous devez faire en sorte que ce mot de passe soit long et complexe, tout en étant facile à retenir.

Chiffrement : processus de conversion d’informations ou de données en code pour les rendre illisibles et inaccessibles.

Complexité (d’un mot de passe) : fait de créer un mot de passe sécurisé. Par exemple, un mot de passe est complexe lorsqu’il mélange des chiffres, des caractères spéciaux (tels que “$” ou “&”), ainsi que des minuscules et des majuscules.

Pirate informatique (ou “hacker”) : personne qui, à l’aide d’un ordinateur, cherche à accéder sans autorisation aux données et aux appareils d’autres entreprises, organisations ou utilisateurs.

Un secret, c'est sacré : Activité 1

Créer un mot de passe sécurisé

Les enfants découvrent comment créer un mot de passe sécurisé et le garder confidentiel.

Objectifs pour les enfants

- ✓ **Mesurer** l'importance de ne jamais communiquer ses mots de passe, sauf à ses parents ou à son tuteur.
- ✓ **Comprendre** l'importance du verrouillage de l'écran pour protéger son appareil.
- ✓ **Apprendre** à créer des mots de passe difficiles à deviner, mais faciles à retenir.
- ✓ **Choisir** le bon système de sécurité pour se connecter, tel que la validation de l'authentification à deux facteurs.

Discussion

Mieux vaut prévenir que guérir

Les technologies numériques nous permettent de communiquer plus facilement avec nos amis, nos proches, nos camarades de classe et les enseignants. Nous pouvons entrer en contact avec eux de multiples façons : par e-mail, par SMS, par messagerie instantanée, ainsi qu'avec des mots, des photos et des vidéos, depuis un téléphone, une tablette ou un ordinateur portable.

Cependant, ces mêmes technologies permettent également aux pirates informatiques et aux fraudeurs de voler plus facilement nos informations et de les utiliser pour endommager nos appareils, altérer nos relations et entacher notre réputation.

Pour nous protéger et protéger également nos informations ainsi que nos appareils, il faut prendre quelques mesures simples : par exemple, verrouiller l'écran de notre téléphone, faire attention aux informations personnelles accessibles sur des appareils déverrouillés (qui peuvent être perdus ou volés) et, surtout, créer des mots de passe sécurisés.

• Qui sait quels sont les deux mots de passe les plus courants ?
(Réponse : "1 2 3 4 5 6" et "motdepasse")

• Quels seraient d'autres exemples de "mauvais mots de passe" ? Pourquoi leur niveau de sécurité n'est pas suffisant ?
(Exemples : votre nom complet, votre numéro de téléphone, le mot "chocolat")

Qui trouve que ce sont de bons mots de passe ? ;)

Activité

Matériels nécessaires :

- Appareils connectés à Internet pour les enfants
- Document intitulé “Consignes pour créer un mot de passe sécurisé”

Voici une suggestion pour créer un mot de passe sécurisé :

- Pensez à une phrase facile à retenir (par exemple, les paroles de votre chanson préférée, le titre d’un livre que vous adorez, une petite phrase dans un film, etc.).
- Choisissez la première lettre ou les deux premières de chaque mot de cette phrase.
- Remplacez certaines lettres par des symboles ou des chiffres.
- Mettez certaines lettres en majuscule et d’autres en minuscule.
- Exercez-vous avec le jeu des mots de passe.

1. Créer des mots de passe

Chacun a 60 secondes pour créer un ou plusieurs mot(s) de passe.

2. Comparer les mots de passe

Chacun écrit en même temps son ou ses mot(s) de passe sur une feuille.

3. Voter

Décidez ensemble quel mot de passe vous semble le plus sécurisé.
Ensuite, discutez-en.

À retenir

Créer un mot de passe sécurisé, c’est non seulement amusant, mais aussi essentiel.

Qu'est-ce qu'un mot de passe sécurisé ?

Voici quelques informations utiles pour créer un mot de passe permettant de protéger vos informations.

Un mot de passe sécurisé est une combinaison de lettres, de chiffres et de symboles. Il peut être tiré d'une phrase facile à retenir mais difficile à deviner, constituée des premières lettres de votre chanson préférée ou de celles de plusieurs mots d'une phrase décrivant une action que vous avez accomplie. Par exemple, la phrase "En 2013, j'étais en classe de CE2 à l'école primaire du centre" peut servir à former le mot de passe "E2013jEcDcE2aLpDc$".

Un mot de passe moyennement sécurisé est difficile à deviner pour les logiciels malveillants, mais pas suffisamment pour une personne qui vous connaît (par exemple, "JeSuisPartiEnItalie").

Un mot de passe peu sécurisé est créé à partir d'informations personnelles, comme le nom de votre animal de compagnie. Il est donc facile à déchiffrer et risque d'être deviné par quelqu'un de votre entourage (par exemple, "JaimeMonpapa" ou "Jaimelechocolat").

À faire

- Utilisez un mot de passe différent pour chacun de vos comptes.
- Utilisez un mot de passe d'au moins huit caractères. Plus il est long, mieux c'est (à condition de vous en souvenir).
- Utilisez une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles.
- Faites en sorte que vos mots de passe soient mémorisables pour que vous n'ayez pas besoin de les écrire quelque part (ce qui peut présenter un risque).
- Changez immédiatement de mot de passe si vous apprenez ou pensez qu'une personne (autre qu'un adulte de confiance) le connaît.
- Utilisez toujours un verrouillage d'écran sécurisé sur vos appareils. Paramétrez vos appareils de sorte qu'ils se verrouillent automatiquement s'ils se retrouvent entre de mauvaises mains.
- Pensez à utiliser un gestionnaire de mots de passe, tel que celui proposé dans votre navigateur, pour mémoriser vos mots de passe. De cette façon, vous pouvez utiliser un mot de passe unique pour chacun de vos comptes, sans avoir à les mémoriser tous.

À ne pas faire

- Ne créez pas votre mot de passe à partir d'informations personnelles (nom, adresse postale, adresse e-mail, numéro de téléphone, numéro de sécurité sociale, nom de jeune fille de votre mère, date de naissance, etc.).
- N'utilisez pas un mot de passe facile à deviner, comme votre surnom, le nom de votre école, votre équipe de rugby préférée, une suite de chiffres telle que 123456, etc. Et surtout, n'utilisez jamais le mot "motdepasse" !
- Ne communiquez votre mot de passe à personne, hormis vos parents ou votre tuteur.
- Ne notez jamais votre mot de passe là où une personne peut le trouver.

Un secret, c'est sacré : Activité 2

Garder son mot de passe secret

Sur un appareil de la maison, montrez aux enfants comment procéder pour personnaliser leurs paramètres de confidentialité.

Objectifs pour les enfants

- ✓ **Personnaliser** les paramètres de confidentialité des services en ligne.
- ✓ **Définir** quelles informations peuvent être partagées ou non sur les sites et les services utilisés.
- ✓ **Comprendre** en quoi consistent l'authentification à deux facteurs ou validation en deux étapes, et quand s'en servir.

Discussion

Quelques éléments d'explication pour vos enfants...

La confidentialité et la sécurité en ligne vont de pair. La plupart des applications et des logiciels offrent des moyens de contrôler quelles informations nous partageons et comment.

Lorsque vous utilisez une application ou un site Web, recherchez l'option intitulée "Mon compte" ou "Paramètres", par exemple. Vous pourrez ainsi accéder aux paramètres de confidentialité et de sécurité pour configurer les actions suivantes :

- Définir quelles informations sont visibles sur votre profil
- Choisir qui peut consulter vos posts, vos photos, vos vidéos ou tout autre contenu que vous partagez

En apprenant à vous servir de ces paramètres pour protéger votre vie privée et en veillant à les tenir à jour, vous contrôlerez plus facilement la confidentialité et la sécurité de vos informations.

Important : Expliquez aux enfants qu'ils doivent toujours définir ces paramètres avec leurs parents ou leur tuteur.

Activité

Matériels nécessaires :

- Appareil connecté permettant de montrer un exemple de compte jugé approprié (par exemple, votre compte email ou celui de l'un de vos enfants)

Étudier ses options

L'appareil choisi est connecté. Accédez à la page des paramètres du site ou de l'app sélectionné(e) par vos soins pour voir quelles sont les options disponibles. Demandez aux enfants comment effectuer les opérations suivantes (le cas échéant) :

- Modifier votre mot de passe
- Accéder à vos paramètres de partage, de localisation et autres pour déterminer lesquels vous conviennent le mieux

- Recevoir des alertes si une personne tente de se connecter à votre compte depuis un appareil inconnu
- Rendre accessible votre profil en ligne (y compris les photos et les vidéos) uniquement aux membres de la famille et aux amis de votre choix
- Activer l'authentification à deux facteurs ou la validation en deux étapes
- Configurer les informations de récupération si vous ne parvenez plus à accéder à votre compte.

Pour déterminer les paramètres de confidentialité et de sécurité qui vous conviennent, expliquer aux enfants d'en parler à leur parents ou tuteur. N'oubliez pas que le paramètre de sécurité le plus important est votre cerveau ! C'est vous qui décidez quelles informations personnelles partager, quand et avec qui.

À retenir

Le choix d'un mot de passe unique et sécurisé pour chacun de vos comptes est une première étape essentielle. À présent, vous devez mémoriser ces mots de passe et les garder pour vous.

Un secret, c'est sacré : Activité 3

Interland : La tour des trésors

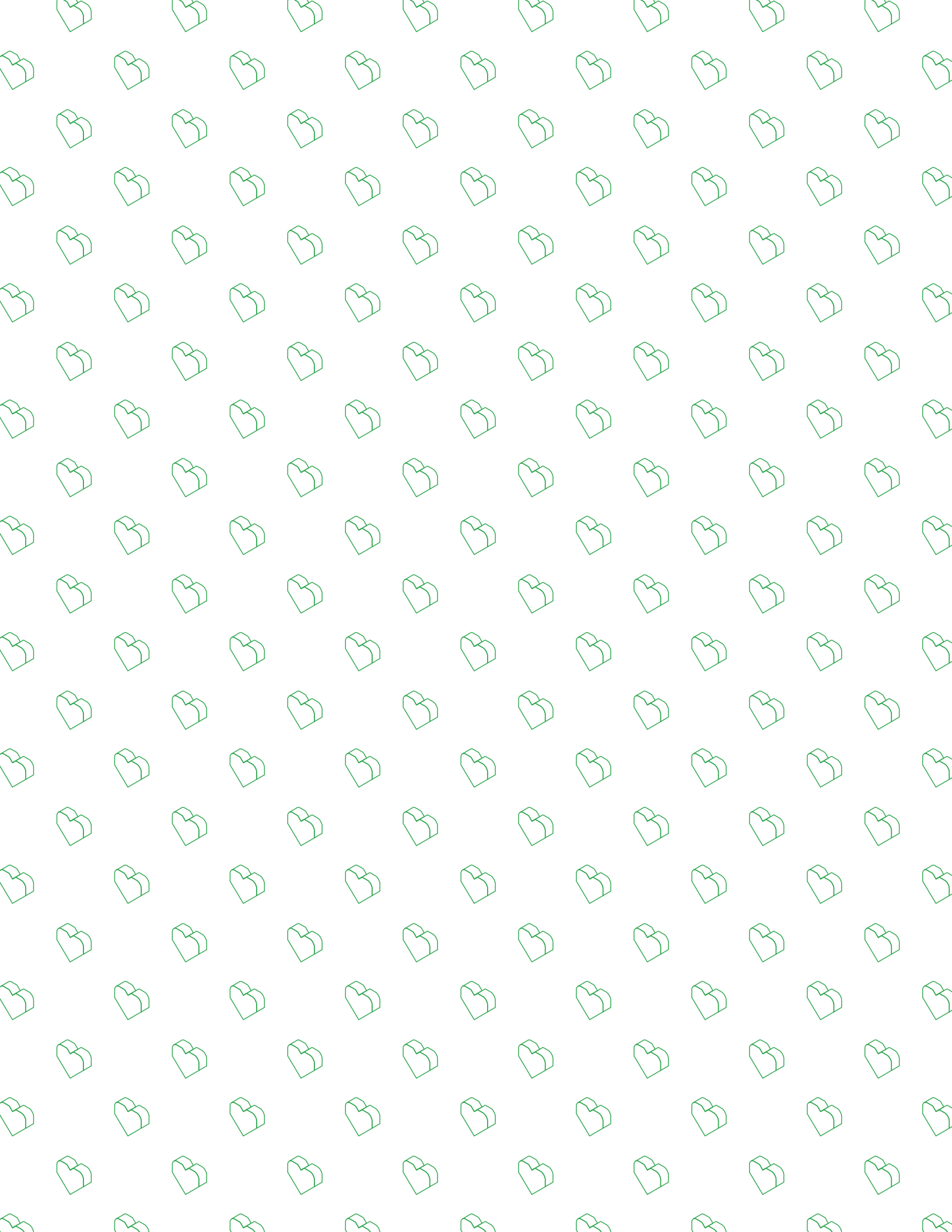
SOS ! La porte de la tour des trésors n'est pas fermée à clé, et toutes les précieuses données des internautes, comme leurs coordonnées et leurs messages privés, sont sans protection. Déjouez le plan néfaste du pirate informatique en bâtissant une forteresse avec des mots de passe sécurisés qui protègent tous vos secrets une fois pour toutes.

Depuis votre ordinateur, ouvrez un navigateur Web et rendez vous sur cybersimple.be/interland.
Accédez ensuite à la tour des trésors.

Sujets de discussion

Invitez les enfants à jouer à "La tour des trésors", puis à répondre aux questions ci-dessous pour discuter des enseignements à tirer de ce jeu.

- Quels sont les critères à respecter pour créer un mot de passe sécurisé ?
- Dans la vraie vie, quand est-il important de créer des mots de passe sécurisés ? Comment vous a-t-on conseillé de procéder ?
- Qu'est-ce qu'un pirate informatique ? Décrivez son comportement et son influence sur le jeu.
- Ce jeu va-t-il changer votre façon de protéger vos informations ?
- Citez une chose que vous feriez différemment après avoir suivi ces thématiques et joué à ce jeu.
- Imaginez trois mots de passe qui répondent aux critères d'un mot de passe sécurisé.
- Citez des exemples d'informations sensibles à protéger.



Thématique 4 : Sois cyber sympa

Être gentil, c'est cool

Avoir un bon comportement en ligne

Aperçu de la thématique

Activité 1 : **Passer à l'action**
Activité 2 : **Maîtriser le ton employé**
Activité 3 : **Joindre le geste à la parole**
Activité 4 : **Interland : Le royaume de la gentillesse**

Thèmes

Le monde numérique pose de nouveaux défis et ouvre de nouvelles perspectives en matière d'interaction sociale, aussi bien pour les enfants que pour l'ensemble d'entre nous. En effet, les codes sociaux peuvent s'avérer plus difficiles à déchiffrer en ligne, la connexion permanente peut être à la fois pratique et anxiogène, et l'anonymat peut susciter autant de comportements positifs que négatifs et nuire à soi comme aux autres.

C'est compliqué, mais nous savons qu'avec Internet, les bons et mauvais comportements peuvent être amplifiés. C'est pourquoi il est essentiel d'apprendre à exprimer de la gentillesse et de l'empathie, tout en sachant comment répondre au harcèlement et aux attitudes hostiles. Cet apprentissage est essentiel pour bâtir des relations saines et réduire le sentiment d'isolement qui conduit parfois au repli, à la dépression, aux difficultés scolaires ou à d'autres problèmes.

D'après une étude, combattre l'intimidation en s'attaquant aux causes sous-jacentes des mauvais comportements est plus efficace que de simplement dire aux enfants de ne pas avoir une attitude incorrecte en ligne. Les activités de cette thématique ont pour but d'inciter les enfants à interagir dès le départ de manière positive et de leur apprendre à gérer les situations où ils sont confrontés à des comportements inadéquats.

Objectifs pour les enfants

- ✓ **Définir** ce qu'est un bon comportement, en ligne et hors connexion.
- ✓ **Interagir** en ligne en adoptant un bon comportement.
- ✓ **Identifier** les situations nécessitant de parler à un adulte de confiance.

Être gentil, c’est cool
Vocabulaire

Harcèlement : comportement délibérément méchant et généralement répété. La personne ciblée a souvent du mal à se défendre.

Cyber harcèlement : harcèlement en ligne ou par le biais d’appareils numériques.

Conflit : dispute ou désaccord qui n’est pas nécessairement répété.

Agresseur : personne à l’origine du harcèlement ou de l’intimidation

Cible : personne victime d’intimidation ou prise pour cible.

Spectateur : témoin du harcèlement ou de l’intimidation, qui constate la situation, mais qui choisit de ne pas intervenir.

Acteur : témoin du harcèlement ou de l’intimidation qui vient en aide à la cible, publiquement ou en privé, parfois en essayant d’arrêter et/ou de signaler l’incident constaté.

Amplifier : accentuer ou encourager la participation ou l’impact.

Exclusion : forme de harcèlement ou d’intimidation en ligne et hors connexion.

Bloquer : action qui consiste à mettre fin à toute interaction avec une autre personne en ligne en l’empêchant, sans l’avertir, d’accéder à votre profil, de vous envoyer des messages, de consulter vos posts, etc. Ce n’est pas toujours idéal, notamment dans les cas d’intimidation où la cible souhaite garder accès à ce que l’agresseur dit ou savoir quand/si l’intimidation a cessé.

Ignorer : action moins définitive que le blocage, qui consiste à ne plus afficher les posts, les commentaires et autres contenus d’une personne dans votre flux de réseau social lorsque ces informations vous ennuient, cela sans avertir cette personne ni être évincé de son flux (pas très utile en cas d’intimidation).

Anonyme : personne sans nom ou inconnue, ou dont vous ne connaissez pas le nom ni l’identité en ligne.

Trolling : posts ou commentaires publiés en ligne avec l’intention délibérée d’être cruel, choquant ou provocateur.

Signaler un abus : action qui consiste à utiliser le système ou les outils en ligne d’un réseau social pour signaler un harcèlement, une intimidation, des menaces et tout autre contenu à caractère nuisible qui ne respectent généralement pas les conditions d’utilisation du service ou les normes de la communauté.

Être gentil, c'est cool : Activité 1

Passer à l'action

Cette activité permet aux enfants d'identifier les quatre rôles-clé d'une situation de harcèlement (l'agresseur, la cible, le spectateur et l'acteur) et de découvrir ce qu'ils peuvent faire s'ils en sont la cible ou les témoins.

Objectifs pour les enfants

- ✓ **Identifier** les situations de harcèlement ou d'intimidation en ligne.
- ✓ **Examiner** ce que signifie être spectateur ou acteur dans ce type de situation en ligne.
- ✓ **Savoir** précisément comment réagir lorsqu'on constate une situation d'intimidation.
- ✓ **Savoir** quelle attitude adopter quand on est victime de harcèlement.

Discussion

Pourquoi être gentil est important?

Gardez bien à l'esprit que derrière chaque nom d'utilisateur ou chaque avatar figure une personne avec de vrais sentiments, qui doit être traitée comme nous voudrions l'être nous-même. Dans une situation d'intimidation ou d'harcèlement, nous trouvons généralement quatre catégories de personnes.

- L'agresseur ou la/les personne(s) à l'origine de l'intimidation.
- La cible, autrement dit la victime de cette intimidation.
- Les témoins des faits (appelés généralement "spectateurs").
- Les témoins des faits qui cherchent à intervenir de façon positive (appelés souvent "acteurs").

Si je suis la cible, j'ai plusieurs possibilités :

- Ne pas répondre.
- Bloquer l'agresseur.
- Informer mes parents, mon professeur, mes frères et sœurs ou toute autre personne de confiance, et utiliser les outils de l'application ou du service concerné qui servent à signaler un post, un commentaire ou une photo qui relève du harcèlement.

Si je suis témoin de harcèlement ou d'un comportement méchant,j'ai la possibilité d'intervenir et de signaler ce comportement. Dans certains cas, les témoins d'une telle situation n'essaient pas de mettre un terme à l'intimidation ni d'aider la cible, mais lorsqu'ils agissent, ils passent du rôle de spectateur à celui d'acteur.

En décidant de ne pas tolérer cette situation et en prônant la gentillesse et la positivité, vous pouvez choisir d'agir. En ligne, un peu de positivité peut faire son effet et contribuer à prévenir les mauvais comportements qui créent de la souffrance.

Si je suis spectateur, je peux devenir acteur de plusieurs façons :

- En trouvant un moyen de montrer ma sympathie envers la personne ciblée ou de l'aider.
- En rédigeant un commentaire ou une réponse pour critiquer le mauvais comportement (mais pas la personne) si vous vous sentez capable de le faire en toute sécurité.
- En décidant de ne pas aider l'agresseur à propager ses propos ou de ne pas aggraver la situation en partageant le post ou le commentaire concerné.
- En demandant à des amis de faire preuve de gentillesse via la publication de nombreux commentaires sympathiques sur la personne ciblée (mais rien de méchant à l'encontre de l'agresseur, car en évitant de riposter, vous donnez l'exemple).
- En signalant le harcèlement à quelqu'un susceptible de vous aider, comme un parent, un enseignant ou un conseiller d'orientation.

Activité

Matériels nécessaires :

- Fiche d'exercice "Passer à l'action"

Réponses pour les différents scénarios :

Scénario 1 : S, A, S (car vous n'aidez pas à améliorer la situation), A, A

Scénario 2 : A, S, A, A

Scénario 3 : A, A, S, S, A

1. Demandez aux enfants de lire les scénarios et de classer les réponses par catégorie

Après avoir décrit les différents rôles, distribuez la fiche d'exercice et accordez 10-15 minutes aux enfants pour lire les trois scénarios et classer chaque réponse par catégorie. Si vous le souhaitez, demandez-leur d'imaginer un quatrième scénario.

2. Discutez des différentes réponses

Avant ou à la fin de la discussion, demandez aux enfants s'ils peuvent expliquer en quoi les personnes qui interviennent dans ces types de situations ont un comportement qui peuvent apporter de l'aide, à l'école et en ligne.

3. Discutez des réponses difficiles à classer par catégories

Demandez aux enfants s'ils ont eu du mal à classer certaines réponses et pourquoi. Discutez-en.

À retenir

Que ce soit en défendant une personne, en signalant un contenu blessant ou en ignorant quelque chose pour empêcher de l'amplifier encore plus, vous disposez de plusieurs options selon la situation. N'importe qui peut faire preuve de gentillesse et contribuer à arranger une situation délicate.

Fiche d'exercice : Activité 1

Passer à l'action

Répétez aux enfants qu'un témoin 'spectateur' peut être utile à la personne victime d'intimidation en devenant un témoin 'acteur'. Vous trouverez ci-dessous trois scénarios qui illustrent différentes situations d'intimidation ou de harcèlement. Si vous le souhaitez, vous pouvez en créer un quatrième à partir d'une situation vécue par quelqu'un que vous connaissez et proposer des solutions du point de vue du spectateur et de l'acteur. Chacun des trois scénarios est déjà accompagné de plusieurs réponses. Lisez-les toutes, puis selon ce que ferait d'après vous un spectateur ou un acteur dans cette situation, ajoutez la lettre S (pour "Spectateur") ou "A" (pour "Acteur") à côté de la réponse correspondante. Discutez ensemble des réponses qui vous ont posé le plus de problème, et expliquez pourquoi.

Scénario 1

Une de vos amies a laissé tomber son téléphone à côté de la fontaine à eau, près du terrain de foot de l'école. La personne qui l'a trouvé a envoyé un message très méchant sur une autre élève à plusieurs camarades de l'équipe de foot avant de reposer le téléphone à côté de la fontaine. L'élève ciblée a alors reproché à votre amie d'avoir envoyé ce message (même si ce n'est pas elle qui l'a fait). Personne ne sait qui en est finalement l'auteur. Que ressentez-vous et que faites-vous ?

- ☐ Vous êtes désolé(e) pour votre amie, mais vous n'intervenez pas, car personne ne sait qui est l'auteur du message.
- ☐ Vous allez voir la personne ciblée pour lui demander de ses nouvelles et si vous pouvez l'aider.
- ☐ Vous propagez l'histoire en partageant le message avec d'autres amis.
- ☐ Vous et votre amie demandez à toute l'équipe de foot de poster des compliments sur la personne ciblée.
- ☐ Vous et votre amie signalez anonymement l'incident à votre chef d'établissement, en lui précisant que tout le monde souhaiterait en savoir plus sur la procédure à suivre pour sécuriser et verrouiller son téléphone.

Scénario 2

Votre professeur a créé un blog pour son cours de langues afin de permettre à sa classe de rédiger des commentaires, de les modifier et de les publier. Le lendemain, elle est malade, et son remplaçant ne remarque pas que la situation commence à mal tourner sur le blog. En effet, une personne publie des commentaires très méchants sur un élève de la classe. Que faites-vous ?.

- ☐ Vous répondez aux commentaires désagréables en disant, par exemple, “C’est pas sympa” ou “Je suis l’ami de _____, et tout ce que tu racontes est faux”.
- ☐ Vous ignorez ces commentaires jusqu’à ce que votre professeur revienne.
- ☐ Vous demandez aux autres élèves d’ajouter de gentils commentaires et des compliments sur l’élève ciblé.
- ☐ Vous signalez au remplaçant qu’une personne se comporte méchamment sur le blog de la classe, et qu’il devrait peut-être en informer votre professeur.

Scénario 3

Plusieurs de vos amis s’amusent beaucoup sur un jeu en ligne. Généralement, les discussions sur le chat du jeu portent surtout sur le jeu lui-même. Cela devient parfois un peu désagréable, mais c’est plus une rivalité amicale que de la vraie méchanceté. Mais cette fois-ci, un joueur commence à tenir des propos vraiment méchants sur l’un de vos amis qui joue, et il n’arrête pas. Il continue même le lendemain. Que faites-vous ?

- ☐ Vous appelez votre ami pour lui dire que la situation ne vous plaît pas et vous lui demandez ce que vous devriez faire tous les deux.
- ☐ Vous appelez tous vos amis qui jouent à ce jeu (en veillant à en informer préalablement votre ami) afin de voir si tout le monde est d’accord pour signaler ces méchancetés.
- ☐ Vous décidez d’attendre pour voir si le joueur cesse d’être méchant, pour ensuite éventuellement agir.
- ☐ Vous décidez de ne plus jouer à ce jeu pendant un certain temps.
- ☐ Vous recherchez les règles de la communauté relatives au jeu pour voir si ce genre de comportement est autorisé, et vous signalez le mauvais comportement à l’aide du système proposé dans le jeu.

Scénario 4

Créez ensemble un scénario à partir d’une situation dont l’un de vous, adulte ou enfant, a entendu parler puis apportez des réponses en distinguant les rôles de spectateur et d’acteur afin de montrer que vous avez bien tout saisi.

Être gentil, c'est cool : Activité 2

Maîtriser le ton employé

Afin d'éviter les situations conflictuelles en ligne, les enfants exercent leur esprit critique en analysant les émotions exprimées à travers des messages instantanés.

Objectifs pour les enfants

- ✓ **Prendre** les bonnes décisions concernant les informations à communiquer, à qui et comment.
- ✓ **Identifier** les situations où il est préférable d'attendre pour discuter en personne plutôt que d'envoyer aussitôt un message.

Discussion

Un malentendu est si vite arrivé

Les petits comme les grands utilisent différents modes de communication pour différents types d'interactions. Cependant, les discussions par chat et par SMS peuvent être interprétées différemment des propos échangés en personne ou par téléphone. Vous est-il déjà arrivé d'être mal compris par message instantané ou par SMS ? Par exemple, avez-vous déjà envoyé une blague à un ami qui l'a prise au sérieux ou qui a même pensé que votre message était méchant ?
Qu'avez-vous fait pour clarifier la communication ? Que pourriez-vous faire différemment ?

Activité

Matériels nécessaires :

- Exemples de messages instantanés, écrits sur une feuille ou sur un appareil connecté

1. Examiner les messages

Étudions ces différents exemples de messages. Si vous en avez de votre côté, écrivez-les pour en discuter.

- "C'est trop cool".
- "Peu importe".
- "APPELLE-MOI MAINTENANT".
- "Très bien".

2. Lire les messages à voix haute

Maintenant, pour chaque message, faites les lire à voix haute par vos enfants sur un ton spécifique (par exemple, 😕 🙃 😀). Que remarquez-vous ? Comment les autres pourraient-ils les prendre ? Comment l'expéditeur de chaque message pourrait-il procéder pour mieux transmettre ce qu'il voulait vraiment dire ?

À retenir

Il n'est pas toujours facile d'anticiper ce que ressent vraiment une personne quand vous lisez son messages. La prochaine fois, veillez à utiliser le bon mode de communication et à ne pas surinterpréter ce que les gens vous disent en ligne. En cas de doute, clarifiez la situation en discutant en personne ou par téléphone avec l'intéressé(e).

Être gentil, c'est cool : Activité 3

Joindre le geste à la parole

Les enfants explorent comment le comportement des adultes peut influencer positivement celui des enfants, et vice versa.

Objectifs pour les enfants

- ✓ **Réfléchir** au comportement en ligne des adultes.
- ✓ **Examiner** les répercussions de l'attitude des adultes sur celle des plus jeunes générations.

Discussion

Les adultes peuvent apprendre aux enfant… et inversement ! Apprendre aux enfants à être gentils est essentiel, mais il est tout aussi important d'appliquer les enseignements que nous dispensons. Nombreux sont les exemples de comportements agressifs et de harcèlement montrant que ces problèmes ne se limitent pas aux enfants. Il suffit de voir comment les adultes se comportent parfois les uns envers les autres, en ligne, dans les médias ou dans les embouteillages.

Nous avons déjà évoqué l'importance d'être gentil avec ses camarades de classe et ses amis, en ligne comme ailleurs. Demandez aux enfants s'ils ont déjà vu des adultes agir méchamment entre eux ou s'intimider mutuellement ? (souvenez-vous que nous ne devons parler que des comportements, sans nécessairement citer de noms)

Demandez leur si leur génération est capable de rendre Internet plus bienveillant et plus positif que les environnements qu'ont créés certains adultes pour eux-mêmes ? (beaucoup d'adultes estiment que les enfants seront probablement meilleurs en la matière)

Demandez leur s'ils pensent que certains enfants intimident les autres ou adressent des commentaires désagréables parce qu'ils reproduisent le comportement des adultes qui les entourent ou des personnes qu'ils voient aux actualités ? Demandez leur en quoi les enfants pourraient être un meilleur modèle pour les adultes ?

À retenir

La façon dont vous et vos amis vous comportez les uns envers les autres aura un impact considérable sur le monde numérique que votre génération construit, et au delà. Chacun a son rôle à jouer !

Être gentil, c'est cool : Activité 4

Interland : Le royaume de la gentillesse

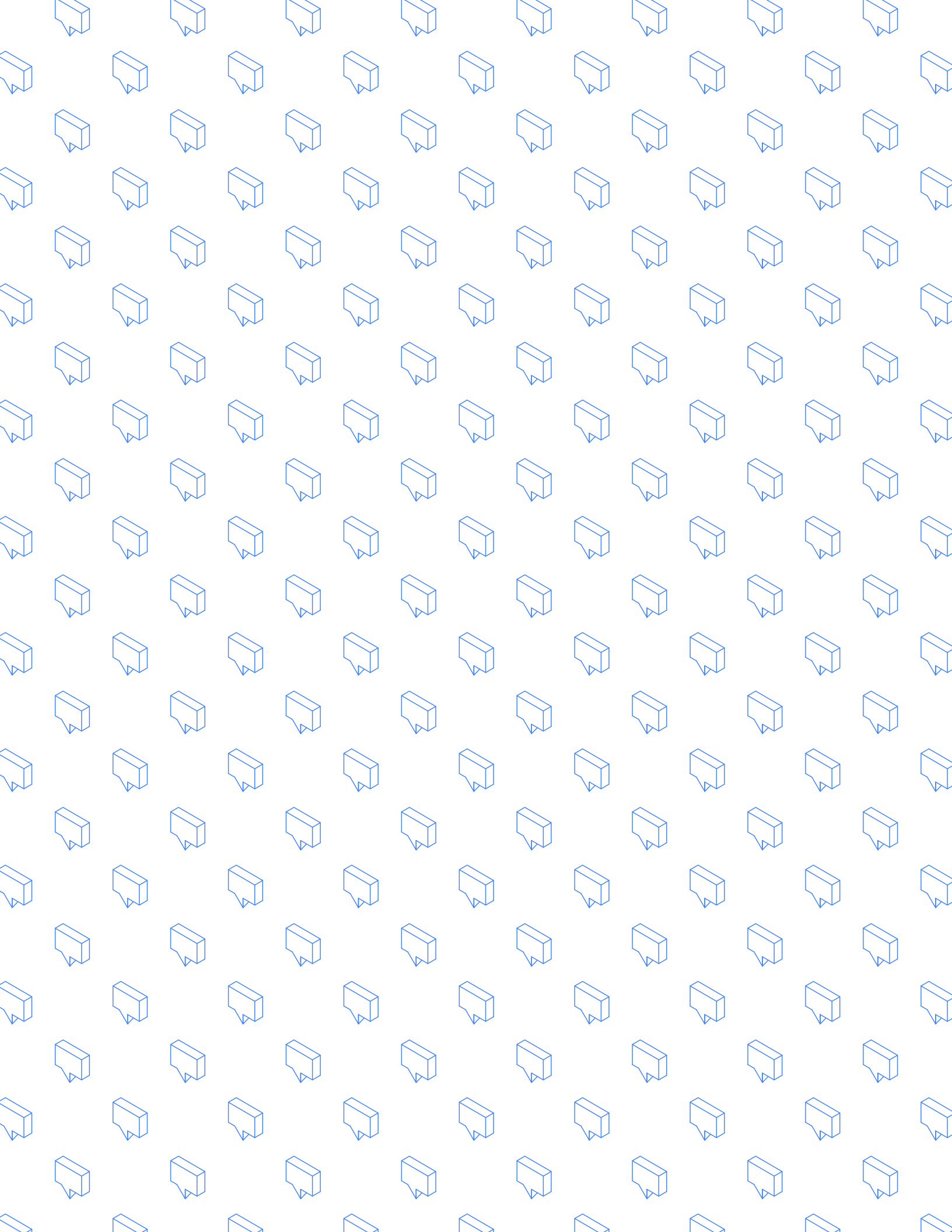
Les émotions de toutes sortes sont contagieuses, pour le meilleur ou pour le pire. Dans le coin le plus ensoleillé de la ville, les agresseurs se déchaînent, propageant des ondes négatives un peu partout. Bloquez ces agresseurs et signalez leur comportement pour les empêcher de prendre le contrôle. Soyez gentils avec les autres internautes afin de rétablir la paix dans cet univers.

Depuis votre ordinateur, ouvrez un navigateur Web et rendez vous sur cybersimple.be/interland.
Accédez ensuite au royaume de la gentillesse.

Discussion

Demandez aux enfants de jouer au "Royaume de la gentillesse" et de répondre aux questions ci-dessous pour discuter ensuite plus en détail des enseignements à tirer de ce jeu.

- Quel scénario du jeu "Le royaume de la gentillesse" vous concerne le plus ? Pourquoi ?
- Décrivez une situation où vous avez agi avec bienveillance envers d'autres personnes en ligne.
- Dans quel cas faudrait-il bloquer une personne en ligne ?
- Dans quel cas faudrait-il signaler le comportement d'une personne ?
- À votre avis, pourquoi le personnage du jeu "Le royaume de la gentillesse" est-il désigné par le terme "agresseur" ? Décrivez ses caractéristiques et comment ses actions affectent le jeu.
- Ce jeu va-t-il changer votre comportement envers les autres ? Si oui, comment ?



Thématique 5 : Sois cyber courageux

En cas de doute, parles-en

Définir et encourager un comportement courageux

Aperçu de la thématique	Activité 1 : **Quand demander de l'aide** Activité 2 : **Signaler le problème en ligne**
Thèmes	Lorsque les enfants sont mal à l'aise en raison d'un contenu en ligne, il est important qu'ils sachent qu'ils ne sont pas seuls, surtout s'ils ont l'impression que quelqu'un d'autre ou eux-mêmes sont susceptibles d'être blessés. Ils ne doivent jamais hésiter à demander l'aide d'une personne de confiance. Il est également utile qu'ils sachent qu'il existe plusieurs façons d'être courageux et de réagir, que ce soit en utilisant les outils de signalement en ligne ou en parlant du problème ailleurs que sur le Web.
Objectifs pour les enfants	✓ **Comprendre** quels types de situations nécessitent de demander de l'aide ou d'en parler avec un adulte. ✓ **Examiner** les options disponibles pour y répondre.

En cas de doute, parles-en
Vocabulaire

Courageux : qui manifeste du courage, sans être nécessairement intrépide, car les gens peuvent être particulièrement courageux et intervenir de manière positive même en cas de peur ou de nervosité.

Compte piraté : compte en ligne dont une autre personne a pris le contrôle et sur lequel vous ne pouvez plus intervenir comme vous le souhaitez.

Pouvoir d'action : ce principe est essentiel à la citoyenneté numérique. Il désigne le fait d'avoir la capacité d'agir ou de faire changer les choses, y compris en assurant sa propre protection ou sa propre défense ainsi que celle des autres.

Confiance : forte conviction que quelque chose ou quelqu'un est fiable et sincère.

En cas de doute, parles-en : Activité 1

Quand demander de l'aide

Tout au long de ces ateliers, un conseil revient régulièrement lorsque les enfants sont confrontés à une situation où ils se sentent mal à l'aise : il faut les encourager à signaler le problème et à faire preuve de courage en s'adressant à quelqu'un de confiance susceptible de les aider, que ce soit vous ou un responsable scolaire. Il est essentiel que les enfants s'en souviennent. Aussi, pour que vous puissiez approfondir le sujet, voici une activité portant essentiellement sur la thématique "en cas de doute, parles-en". Vous trouverez ci-après différentes situations où parler d'un problème peut vraiment être utile.

Remarques importantes

1. Depuis des générations, les enfants sont éduqués et conditionnés de façon à ne pas "rapporter", au point que cela soit devenu une norme sociale. Aujourd'hui, les experts en prévention du harcèlement scolaire s'efforcent d'expliquer aux enfants la différence entre "rapporter" et demander de l'aide. Vous devez faire comprendre aux enfants que demander de l'aide lorsqu'une situation en ligne les met mal à l'aise ne revient pas à "rapporter", mais qu'il s'agit d'obtenir de l'aide pour eux-mêmes comme pour leurs camarades lorsque des personnes sont blessées.

2. Encouragez les enfants à parler ouvertement et rappelez-leur que vous restez à leur disposition pour leur offrir votre soutien s'ils décident d'intervenir, ou pour leur expliquer comment signaler un problème de manière adéquate.

3. Lors de la discussion ci-dessous, chaque fois qu'un enfant raconte une situation où il a sollicité l'aide d'un adulte, faites en sorte que le ton de la conversation le rende fier et mette en avant son courage d'être intervenu.

Objectifs pour les enfants

- ✓ **Prendre** conscience que demander de l'aide pour soi-même ou pour d'autres est un signe de force.
- ✓ **Réfléchir ensemble et à voix haute** aux situations où il peut vraiment être utile d'en parler.

Discussion

Voici différentes situations dans lesquelles chacun est susceptible de se retrouver en ligne. Demandez à vos enfants s'ils ont déjà connu l'une d'entre elles afin qu'ils racontent comment ils ont réagi, pour ensuite en discuter tous ensemble.

Sujets de discussion

Demandez à vos enfants de lire en silence les scénarios ci-dessous. Demandez leur en même temps s'il se sont déjà retrouvés dans l'une de ces situations, s'ils voulaient solliciter l'aide d'un adulte, et s'ils l'ont fait ou non et pourquoi.

- Tu as eu l'impression que ton compte avait peut-être été piraté. (discussion possible : que peut-on faire pour renforcer la sécurité d'un compte en ligne ?)
- Tu as eu besoin d'aide pour te souvenir d'un mot de passe.
- Tu n'as pas vraiment su si tu avais affaire à une escroquerie et tu t'es demandé si tu es tombé dans le panneau. (discussion possible : quels sont les signes à repérer ?)
- Quelqu'un a voulu te parler en ligne de quelque-chose qui t'a mis mal à l'aise.
- Tu as reçu un message ou un commentaire suspect d'un inconnu. (discussion possible : à quoi reconnait-on un message suspect ?)
- Tu as voulu parler avec un adulte d'une chose vraiment gentille OU vraiment très méchante que quelqu'un a dite en ligne.
- Tu as partagé quelque chose en ligne tu n'aurais peut-être pas dû transmettre et cette situation t'as tracassé.
- Tu as été témoin d'une situation où un camarade a été blessant vis-à-vis d'un autre enfant en ligne.
- Tu as vu une personne menacer quelqu'un de se battre ou de lui faire du mal.
- Quelqu'un a publié un faux profil en se faisant passer pour un ami.
- Un post ou un message d'un autre enfant vous a tracassé.

À retenir

Ce n'est peut-être pas toujours évident, mais être capable de demander de l'aide lorsque vous ne savez pas vraiment quoi faire est une vraie preuve de courage. Que ce soit pour faire cesser un mauvais comportement ou pour mettre un terme aux souffrances que vous ou quelqu'un d'autre subissez, cette démarche est aussi valeureuse qu'intelligente.

L'assistance téléphonique de Child Focus est accessible à tous les adultes ou enfants souhaitant trouver de l'aide pour une jeune personne en situation de détresse. Si possible, gardez le numéro de Child Focus bien en vue à la maison et rappelez à votre enfant qu'il/elle peut appeler le 118 0000 si quelque chose de grave se passe et qu'il/elle n'ose pas en parler avec vous, un professeur ou un proche.

En cas de doute, parles-en : Activité 2

Signaler un problème en ligne

À l'aide d'appareils de la maison (pour voir concrètement comment signaler un contenu ou un comportement inapproprié dans des applications), les enfants examinent différents types de contenus et décident si ces derniers doivent être signalés ou non en justifiant à chaque fois leur choix.

Objectifs pour les enfants

- ✓ **Connaître** les outils en ligne pour signaler un abus.
- ✓ **Déterminer** quand les utiliser.
- ✓ **Savoir** pourquoi et quand signaler un abus.

Discussion

Qu'il s'agisse de méchancetés ou de contenus inappropriés en ligne, plusieurs options sont possibles pour intervenir. Lors de l'activité précédente, nous avons évoqué la plus importante qui consiste à parler du problème à un adulte de confiance. Une autre option est de le signaler dans l'application ou le service concerné pour que le contenu puisse être éventuellement supprimé.
Il est important que chacun ait le réflexe d'utiliser les outils de signalement en ligne. Par ailleurs, avant d'utiliser des outils de blocage et de signalement, les enfants doivent prendre l'habitude de faire une capture d'écran de la conversation ou de l'activité blessante ou suspecte afin de garder une trace du problème. De cette façon, les adultes de confiance peuvent voir ce qui s'est passé et aider à le résoudre.

Activité

Matériels nécessaires :

- Fiche d'exercice "Signaler le problème en ligne"

1. Connaître la procédure à suivre pour signaler un problème
Rassemblez le maximum d'appareils accessibles à la maison. Recherchez ensemble les outils permettant de signaler un contenu ou un comportement inapproprié dans au moins trois interfaces ou comptes différents.

2. Lire chaque situation
Étudiez ensemble les sept situations décrites sur la fiche d'exercice.

3. Quels contenus signaler...
Demandez à vos enfants s'ils auraient signalé le contenu ou non.

4. ... Et pour quelles raisons ?
Demandez aux enfants d'expliquer leur choix. Il y a rarement une seule bonne réponse ou approche. Assurez-vous que les enfants en soient bien conscients avant d'engager la discussion.

À retenir

La plupart des applications et des services proposent des outils pour signaler et/ou bloquer les contenus inappropriés. Ces outils ont l'avantage de permettre d'aider les personnes touchées, leur communauté, ainsi que les plates-formes elles-mêmes. Avant de bloquer ou de signaler ce type de contenu, il est toujours prudent de faire une capture d'écran afin de garder une trace du problème.

Fiche d'exercice : Activité 2

Signaler un problème en ligne

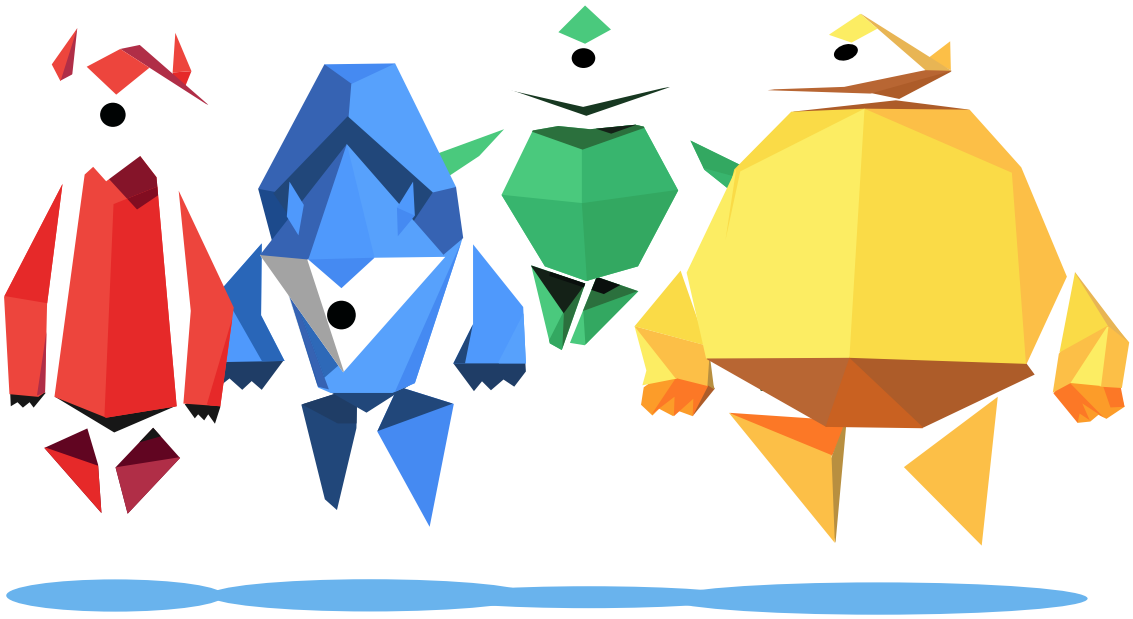
Lisez chaque situation, puis levez la main si vous la signaleriez dans l'application ou le service utilisé. Préparez vous à expliquer pourquoi vous le feriez ou non, ainsi que la raison pour laquelle vous opteriez pour cette option. Discutez-en ensuite tous ensemble.

Remarques importantes

Tous doivent être conscient qu'il existe rarement une seule solution, d'où l'utilité de cette discussion. Personne ne doit s'en vouloir d'avoir fait tel ou tel choix. Même les adultes ne savent pas toujours quand ou comment signaler un problème.

Situation 1	Un enfant publie une photo de groupe via un compte public, et vous détestez la tête que vous avez dessus. Signaleriez-vous cette photo ou non ? Comment pouvez-vous intervenir ?
Situation 2	Une personne a créé un compte en utilisant le nom et la photo d'un enfant que vous connaissez. Elle a transformé cette photo en mème et dessiné une moustache ainsi que d'autres motifs bizarres pour en faire au final une photo ridicule. Signaleriez-vous ce compte ou non ?
Situation 3	Quelqu'un a publié de nombreux commentaires méchants sur un enfant de votre école de manière anonyme, mais vous pensez savoir de qui il s'agit. Signaleriez-vous ces commentaires ou non ?
Situation 4	Un ami a créé un compte avec le nom de votre école en pseudonyme, et publié des photos d'enfants accompagnées de remarques dont tout le monde a entendu parler. Certains commentaires sont méchants, d'autres sont des compliments. Signaleriez-vous les commentaires méchants, tout le compte, ou les deux ?
Situation 5	Un soir, vous remarquez qu'une copine a indiqué dans un commentaire qu'elle allait se battre le lendemain à la cantine avec un autre. Signaleriez-vous ce commentaire en ligne ou non ? Devriez-vous en informer un enseignant ou le chef d'établissement le lendemain matin ou pas ? Ou faire les deux ?
Situation 6	Vous regardez un dessin animé jusqu'à ce qu'un contenu pas du tout adapté aux enfants s'affiche soudainement et vous mette mal à l'aise. Signaleriez-vous le problème ou non ?
Situation 7	Vous jouez à un jeu en ligne avec des amis, et une personne qu'aucun joueur ne connaît se met à discuter avec vous. Elle n'est pas méchante ni quoi que ce soit, mais vous ne la connaissez pas. Devriez-vous l'ignorer ou la signaler ?

BONUS



BONUS

Dessine la carte des écrans à la maison

Combien y a-t-il d'écrans à la maison ? Quels sont leurs usages quotidiens ? Cette première activité permet de dresser un état des lieux des objets connectés à la maison et de réfléchir à vos relations aux écrans en famille. Il s'agit d'un premier pas vers la citoyenneté numérique.

Temps de préparation:
- 5 minutes de discussion et de lancement avec les adultes
- 1 heure d'activité pour les enfants

Objectifs des enfants

- ✓ **Explorer** les usages possibles des médias connectés
- ✓ **Adopter** un regard critique sur vos relations aux écrans
- ✓ **Questionner** les effets des technologies sur la santé et sur les relations avec les autres
- ✓ **Laisser** aller sa créatvité
- ✓ **Structuration et vision** de l'espace

Activité

Ressources nécessaires :

- Une feuille la plus grande possible A2/A3 ou plusieurs feuilles A4 à rassembler.
- Feuilles de brouillons
- Feutres et crayons
- Colle et ciseaux (optionnel)

1. Commencer par dresser un inventaire

Combien d'écrans y a-t-il à la maison ?
Pourquoi vous servez-vous de cet écran ?
Voici un tableau pour s'inspirer :

Ecrans	Pour qui et pour quoi faire ?
1 Ordinateur	Pour travailler (Maman) Pour jouer (enfant 1) Pour chercher de l'information (enfant 2) ...
1 Tablette	Lire le journal (Papa) ...
3 Smartphones	Communiquer (Whatsapp, Instagram...) Ecouter de la musique
1 Télévision	Se divertir S'informer

Il est possible d'avoir des réponses différentes selon les membres de la famille. Dans ce cas, utilisez une couleur pour chacun des membres.

Discutez ensuite des différentes utilisations : certains prennent l'ordinateur uniquement pour travailler, d'autres se servent du téléphone juste pour appeler et communiquer et d'autres pour jouer.
Y a-t-il des limites de temps pour l'un ou l'autre écran ?
Y a-t-il des moments où les écrans sont interdits ?

2. Construire votre carte

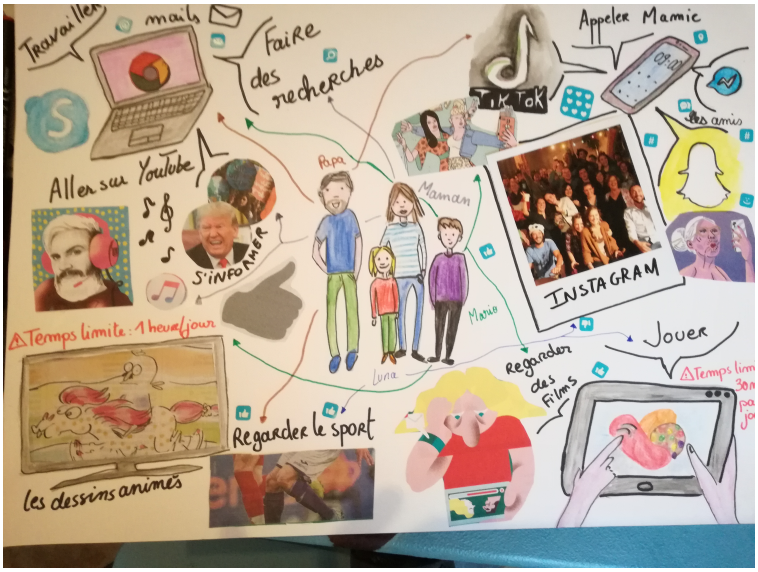
Sur la grande feuille, dessinez au centre votre famille ou votre maison ou coller une photo.
Représentez ensuite chaque écran dans un coin de la feuille.

Continuer à la page suivante →

Autour de chaque écran, dessinez ou écrivez les usages possibles que vous avez listé. Vous pouvez insérer des photos, des smileys, des logos des réseaux sociaux, moteurs de recherche, etc. Soyez créatifs !
Reliez ensuite chaque membre de la famille avec une couleur aux différents écrans qu'il utilise et ses usages.

Il est possible d'ajouter les règles de limites de temps pour chaque écran et/ou des phrases plus personnelles sur du ressenti, sur ce que chacun aime ou n'aime pas (ex : *« j'aime jouer sur mon GSM, ça me détend. »*, *« je n'aime pas l'ordinateur car je n'y comprends rien »,* etc.) Voilà, votre carte mentale des écrans est prête ! Plus elle sera colorée et amusante, plus vous aurez envie de l'afficher chez vous.

Exemple



N'hésitez pas à nous envoyer votre carte des écrans par mail (cyberheros@bibliosansfrontieres.be), nous les partagerons sur nos réseaux sociaux !

Ce contenu est proposé par Bibliothèques Sans Frontières Belgique