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”) : manipulation en croyant qu’ils s’adressent à une vraie personne ou à une page légitime en ligne en croyant qu’ils s’adressent à une vraie personne ou à une page légitime. l’attention des internautes et les inciter à cliquer sur un lien ou une page Web, souvent pour augmenter le nombre de vues ou le trafic sur un site et gagner ainsi de l’argent.

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'ils peuvent s'adresser à un adulte de confiances'ils pensent être victimes 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 ?

Continuer à la page suivante →

- 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 vert 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).

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 risquera de s'aggraver.

Activité

Matériel nécessaire :
- Fiche d'exercice *Exemples d'hameçonnage*

1. Étudier les exemples
Etudiez avec vos enfants les différents exemples de messages et de sites Web fournis.

2. Indiquer 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. Discuter 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. Continuer 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 ?
- **Vous propose-t-on quelque chose de gratuit ?**
  Les offres gratuites ne sont généralement jamais vraiment gratuites.
- **Est-ce que l'on vous demande des informations personnelles ?**
  Certains sites Web vous demandent des informations afin de vous envoyer encore

Continuer à la page suivante →

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.** L'URL est suspecte et n'est pas 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.

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.

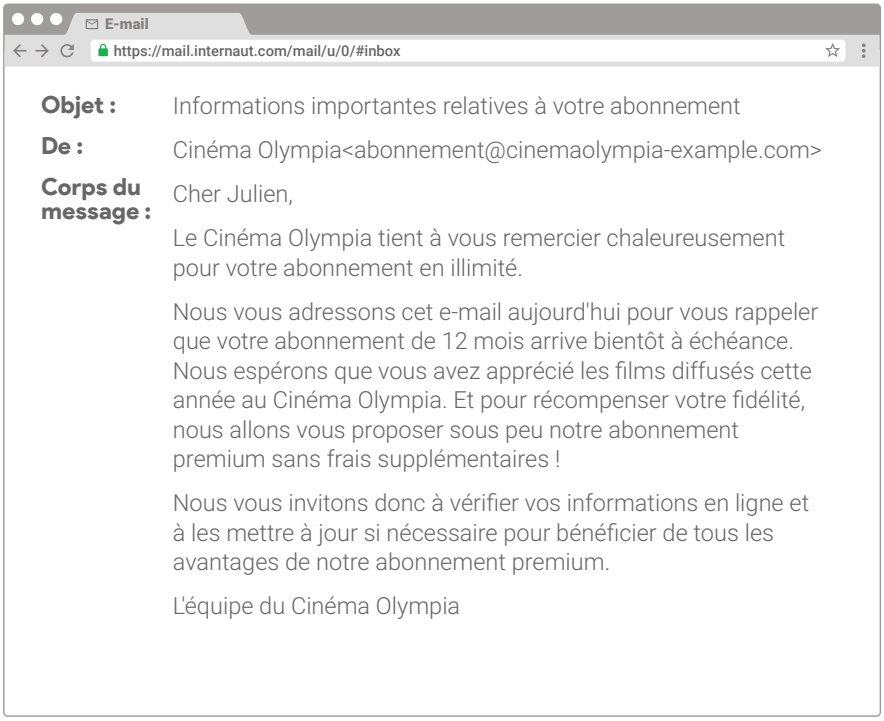
Remarque : pour les besoins de cet exercice, partez du principe que la messagerie Internaute est fiable.

Conclusion

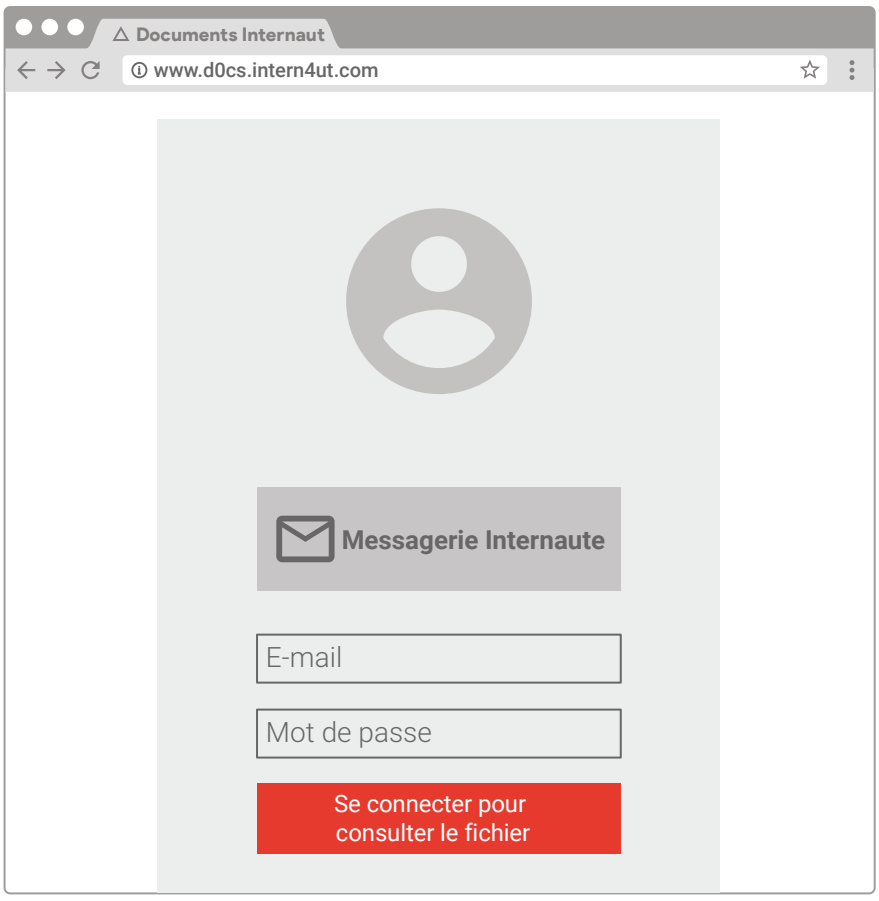
Lorsque vous êtes en ligne, faites toujours attention aux tentatives d'hameçonnage par e-mail, par SMS ou dans les posts. Et si vous vous faites berner, avertissez immédiatement un adulte en qui vous avez confiance.

Fiche d’exercice – Activité 1

Exemples d’hameçonnage

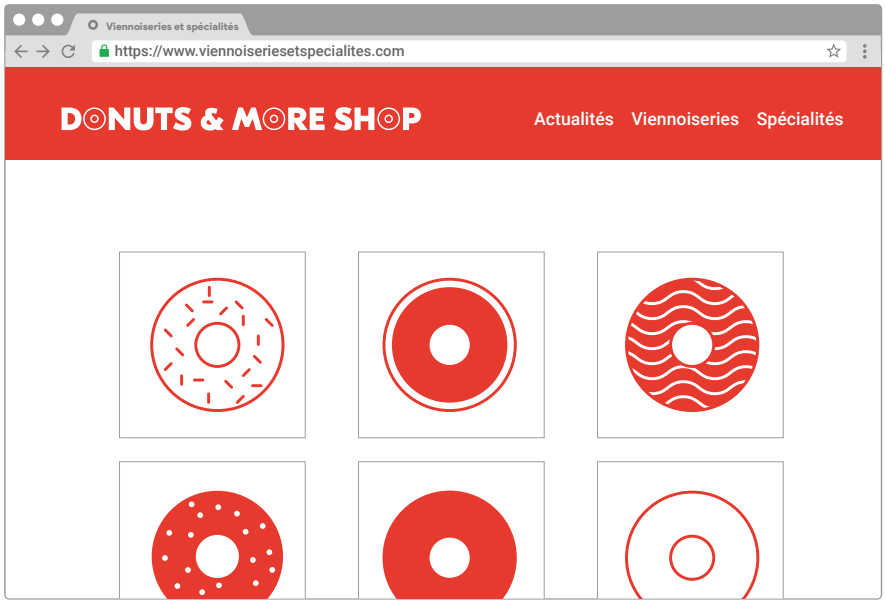


1. Ce message est-il fiable ou est-ce un cas de hameçonnage ?

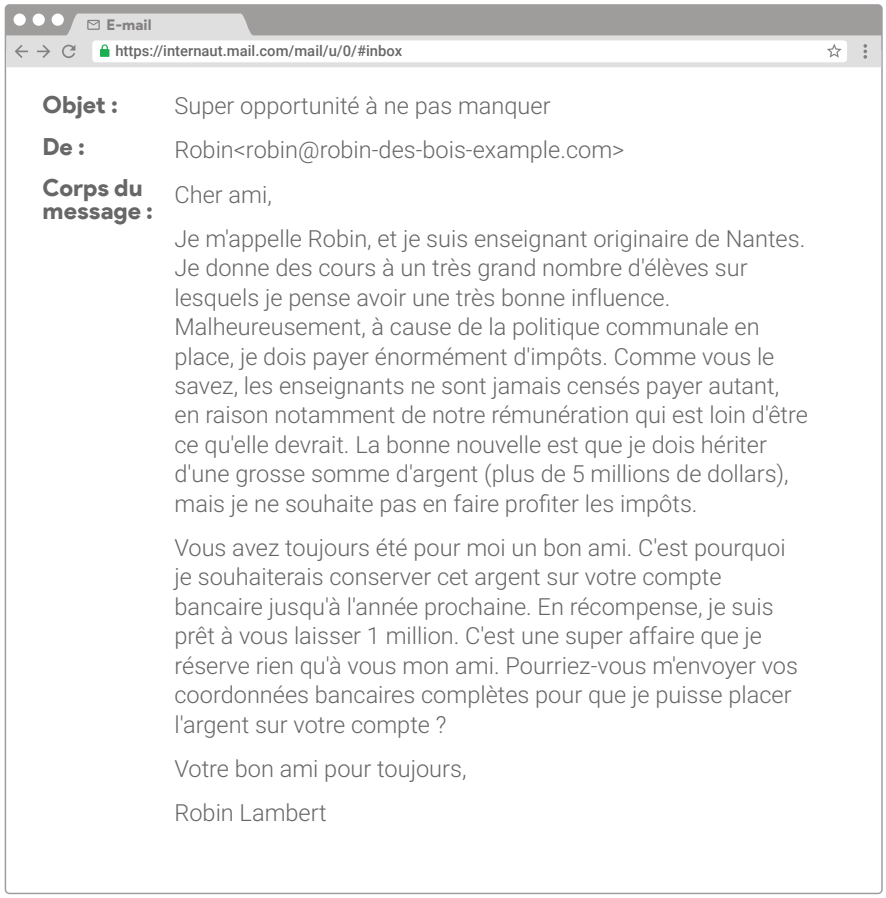


2. Cette page est-elle fiable, ou est-ce un cas de hameçonnage ?

Continuer à la page suivante →

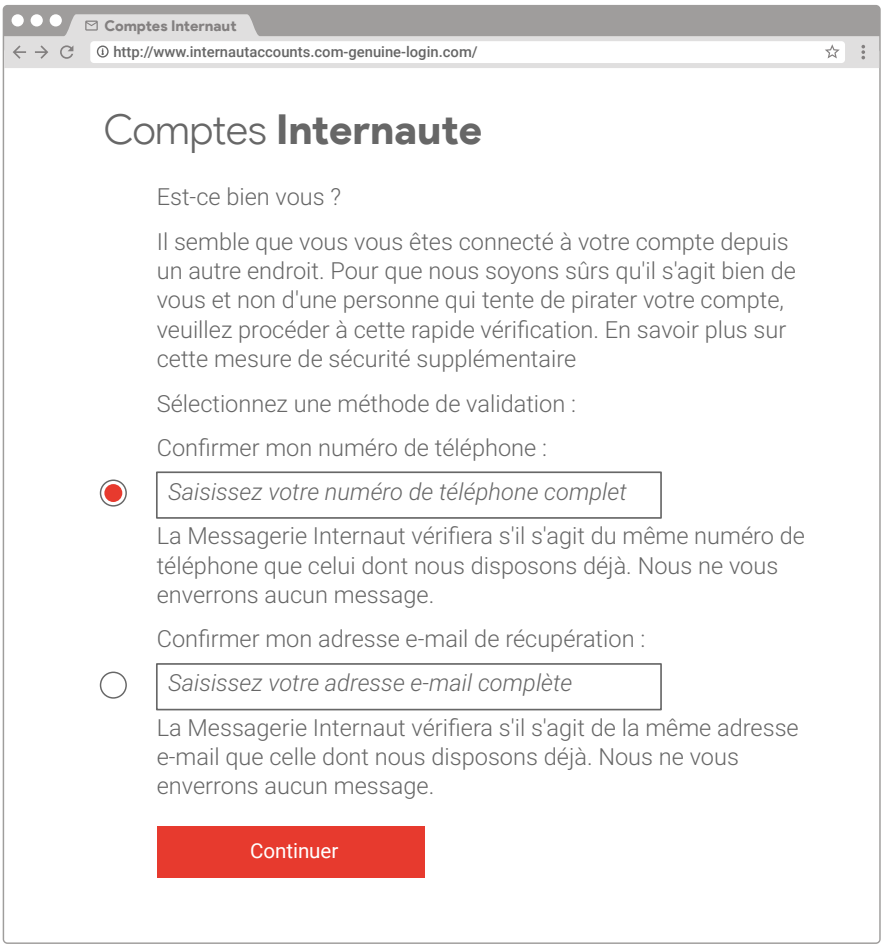


3. Ce site est-il fiable ou s'agit-il d'une escroquerie ?



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

Continuer à la page suivante →



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 avec eux. La solution la plus sûre est de ne pas répondre ou d'avertir un parent ou un adulte de confiance que l'internaute en question tente de communiquer avec vous. 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.

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 ?

Continuer à la page suivante →

- **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.

Étudiez un ou plusieurs scénarios et expliquez comment 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.

Conclusion

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.
- **"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.

Continuer à la page suivante →

- **“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 !
- **“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 06 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.
- **“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.
- **“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.
- **“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.
- **“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.

Continuer à la page suivante →

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.
- **“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 élèves 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

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.

Conclusion

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 ou votre appareil mobile (une tablette, par exemple), ouvrez un navigateur Web et rendez-vous sur https://beinternetawesome.withgoogle.com/fr_be/interland/destination/reality-river.

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 tirer de ce jeu.

- 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 ?