## 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.

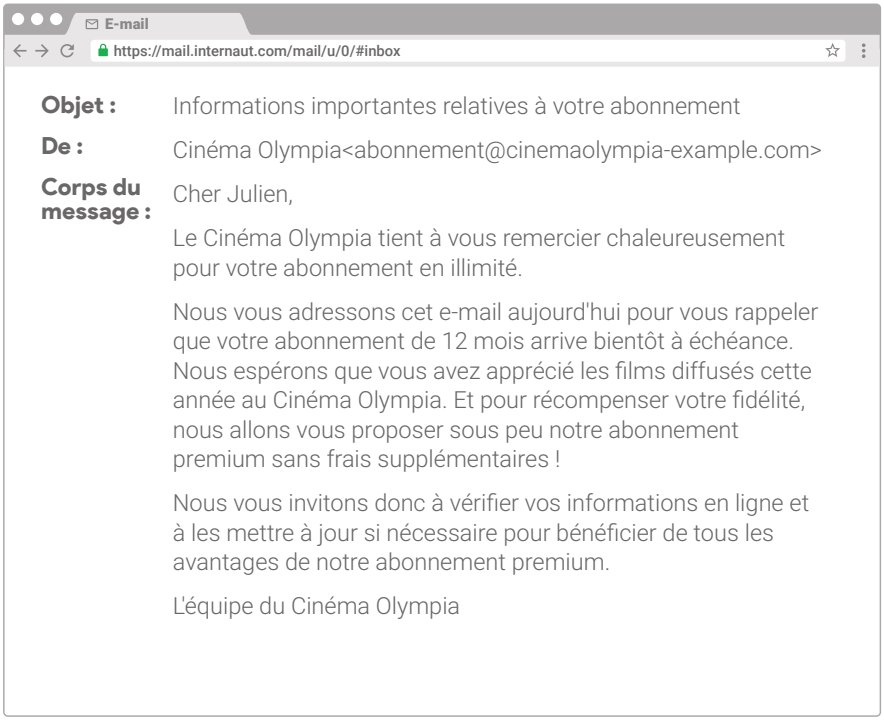
*Remarque : pour les besoins de cet exercice, partez du principe que la messagerie Internaute est fiable.*

## Conclusion

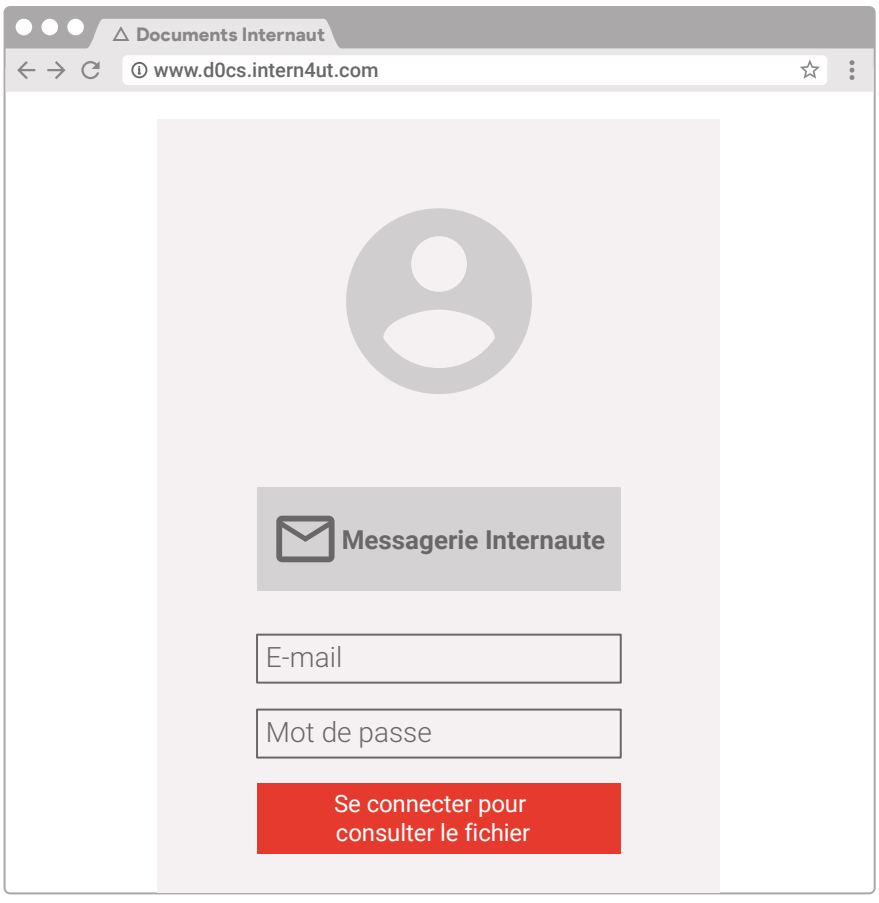
Lorsque vous êtes en ligne, faites toujours attention aux tentatives d'hameçonnage par e-mail, par SMS ou dans les posts. Et si vous vous faites berner, avertissez immédiatement un adulte en qui vous avez confiance.

## Fiche d’exercice – Activité 1

# Exemples d’hameçonnage

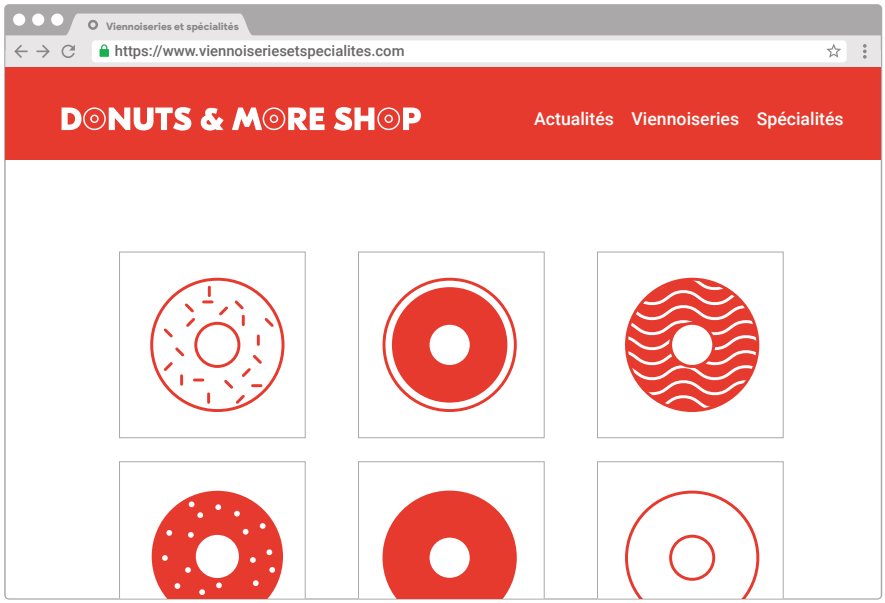



**1. Ce message est-il fiable ou est-ce un cas de hameçonnage ?**

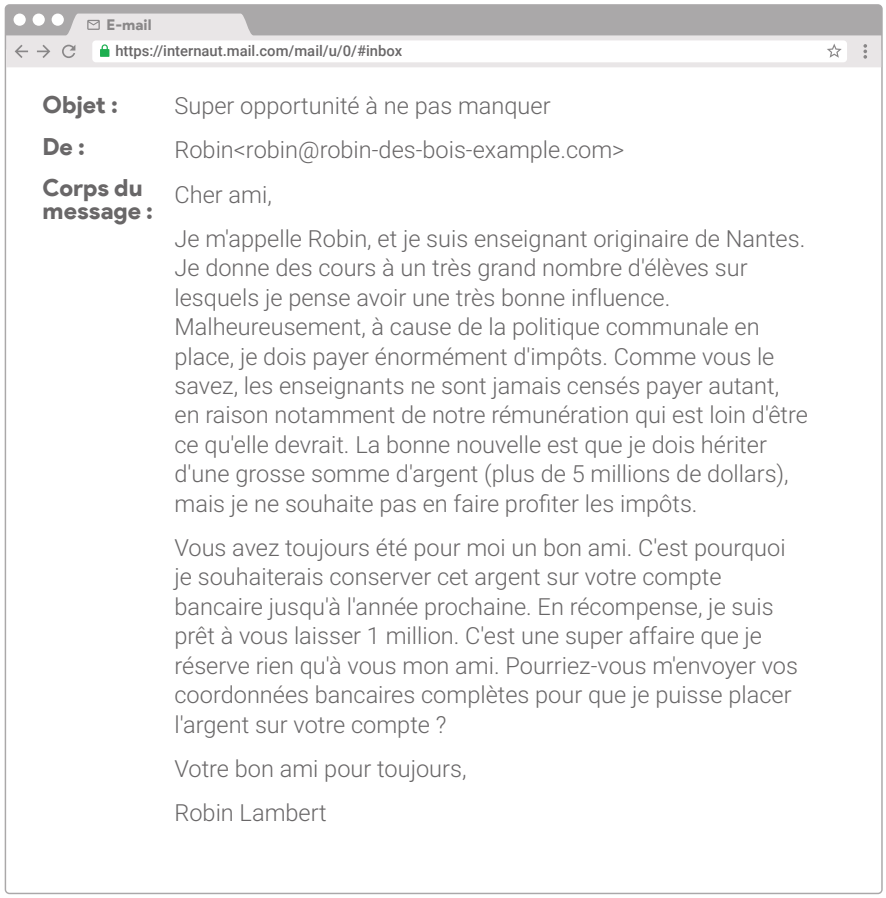



**2. Cette page est-elle fiable, ou est-ce un cas de hameçonnage ?**

Continuer à la page suivante →

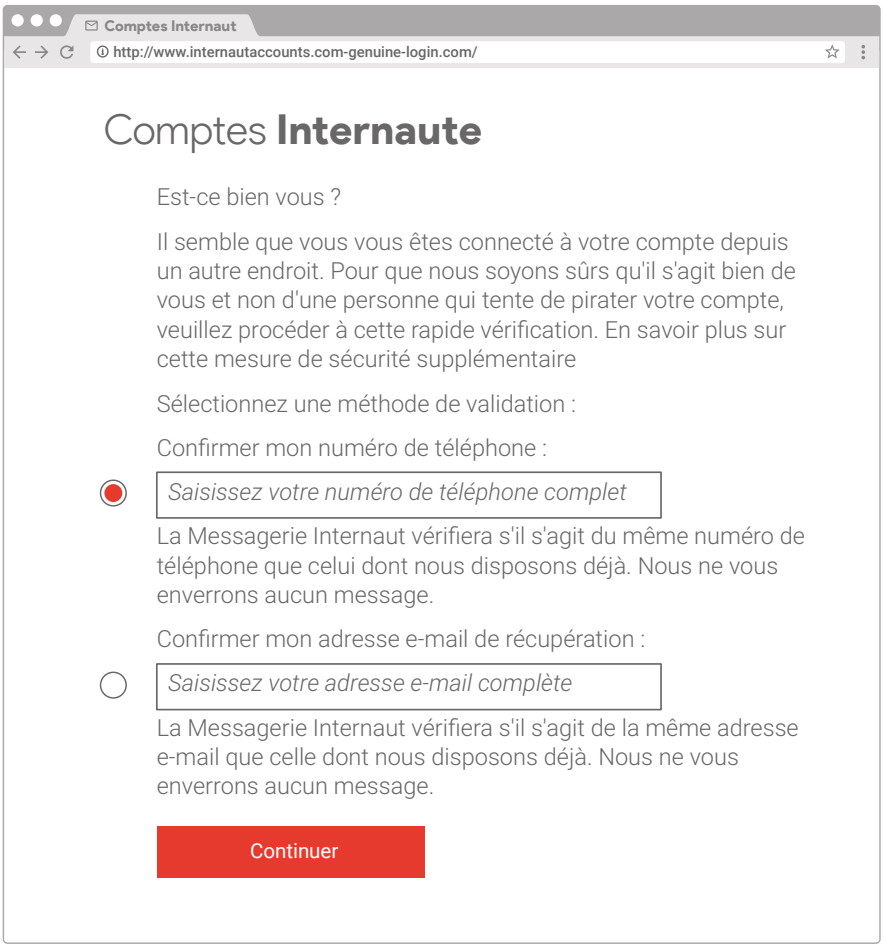



## 3. Ce site est-il fiable ou s'agit-il d'une escroquerie ?




## 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 ?