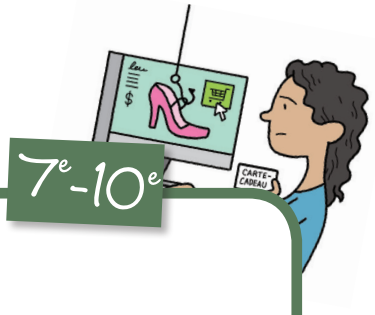
IDENTITÉ CITOYENNETÉ NUMÉRIQUE

Ne mordez pas à l'hameçon!



Objectif

L'objectif est d'outiller les élèves afin qu'elles et ils puissent reconnaître et éviter les tentatives d'hameçonnage et les tentatives d'interception et de vol des données.

Résultats d'apprentissage

Les élèves seront en mesure :

- de développer leur esprit critique quant à l'échange de renseignements personnels sur Internet;
- d'adopter des stratégies afin de reconnaître les tentatives d'hameçonnage;
- de prendre les mesures nécessaires pour assurer la sécurité de leurs renseignements personnels et de leur information bancaire après avoir été victime d'hameçonnage;
- de signaler les tentatives d'hameçonnage auprès des autorités.

Glossaire

Hameçonnage : Technique frauduleuse utilisée par des gens malhonnêtes voulant obtenir des renseignements personnels et bancaires afin d'usurper l'identité de la victime.

Renseignements personnels : Ensemble des renseignements qui pourraient servir à identifier une personne (p. ex., nom, date de naissance, adresse).

Usurpation d'identité : Tromperie par laquelle une personne se sert de renseignements personnels obtenus frauduleusement pour se faire passer pour une autre personne; l'objectif est souvent d'accéder aux comptes de banque de la personne dont l'identité a été usurpée.

ACTIVITÉS SUGGÉRÉES

ACTIVITÉ DE REMUE-MÉNINGES

Indices d'hameçonnage

(Groupes/Individuel)

Marche à suivre

1. Animer un remue-méninges pour déterminer les indices ou critères que les élèves utilisent pour évaluer si un courriel est une tentative d'hameçonnage.
2. Poser aux élèves la question suivante : Quels indices ou critères utilisez-vous pour déterminer si un courriel est une tentative d'hameçonnage?
3. Noter les résultats du remue-méninges sur une grande feuille, au tableau ou dans un document de collaboration en ligne afin que les élèves puissent tous et toutes consulter les réponses.
4. Au besoin, compléter la liste à partir des éléments de réponse suggérés à l'annexe **Indices d'hameçonnage – Éléments de réponse** (voir Annexe A).
5. Animer une discussion de classe pour permettre aux élèves de faire part de leurs expériences avec les tentatives d'hameçonnage.

ACTIVITÉS SUGGÉRÉES

ANALYSE D'UN COURRIEL HAMEÇON

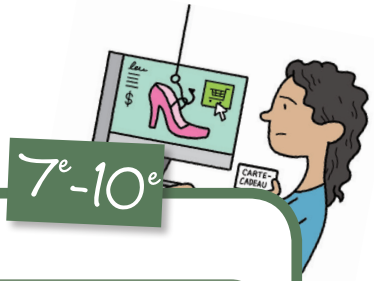
Indices d'hameçonnage

(Groupes/Individuel)

Marche à suivre

1. Photocopier la **Fiche d'analyse d'un courriel hameçon** (voir Annexe B) ainsi que l'**Exemple de courriel hameçon** (voir Annexe C) pour chaque élève ou groupe d'élèves.
2. Distribuer les documents et demander aux élèves de noter, sur la **Fiche d'analyse d'un courriel hameçon** (voir Annexe B), les indices qui servent à déterminer que l'exemple de courriel hameçon (voir Annexe C) est une véritable tentative d'hameçonnage.
3. Après que les élèves ont terminé leur analyse, faire la mise en commun des résultats du groupe.

Ne mordez pas à l'hameçon!



ACTIVITÉS SUGGÉRÉES

DISCUSSION

Tentatives d'hameçonnage – Que faire?

(Groupe-classe/Groupes)

Marche à suivre

1. Revoir la liste d'indices écrits au tableau pour déterminer si l'activité d'analyse du courriel hameçon a permis aux élèves de trouver des nouveaux indices.
2. Animer une discussion de groupe et demander aux élèves de réfléchir aux questions suivantes :
   a. Avant d'entrer ses renseignements personnels sur un site Web, quelles stratégies pourrait-on utiliser pour confirmer qu'un site est légitime et digne de confiance?
      - Éléments de réponse : Entrer les adresses URL du site Web manuellement au lieu de cliquer sur les liens qui se trouvent dans un courriel suspect; vérifier si l'adresse du site Web débute par « https:// »; vérifier si une icône de cadenas fermé ou de clé non brisée est visible dans la barre d'adresse du navigateur Web.

   b. Que peut-on faire pour confirmer l'état d'un compte auprès d'un marchand ou d'une entreprise après une tentative d'hameçonnage?
      - Éléments de réponse : Accéder au véritable site Web du marchand ou de l'entreprise en question à partir d'un nouvel onglet et non à partir de liens qui se trouvent dans le courriel hameçon; vérifier l'état d'un compte en communiquant directement avec le marchand en composant le numéro de téléphone qui se trouve sur le véritable site Web du marchand ou de l'entreprise.

   c. Quelles stratégies pourrait-on adopter pour éviter de se laisser prendre à l'hameçon?
      - Éléments de réponse : Utiliser un antivirus; filtrer les courriels indésirables; ne jamais répondre aux courriels réclamant des renseignements personnels; surveiller les transactions dans ses comptes afin de s'assurer qu'elles sont toutes valides.

   d. Au Canada, à qui devrait-on signaler les tentatives d'hameçonnage?
      - Éléments de réponse : Afin de signaler un courriel qui semble être une tentative d'hameçonnage, on doit le faire suivre au Centre antifraude du Canada (CAFC) à l'adresse info@centreantifraude.ca. C'est l'organisme canadien qui se charge de renseigner le public en documentant les tentatives de fraudes.

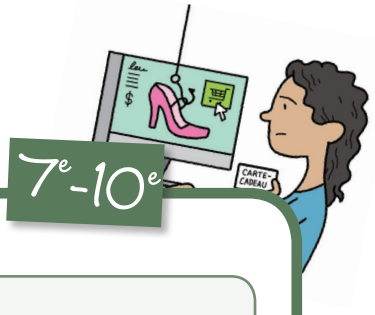
   e. Que faire si l'on est victime d'hameçonnage?
      - Éléments de réponse : Après avoir été victime d'hameçonnage, on doit communiquer avec les autorités et son institution financière. Il est essentiel de mettre à jour son information bancaire. De plus, on doit changer ses mots de passe. On doit aussi vérifier son ordinateur à l'aide d'un logiciel antivirus. Il est essentiel de déterminer si des logiciels malveillants ou des logiciels espion ont été téléchargés à partir des sites Web frauduleux qui ont été visités en cliquant sur les liens d'un courriel hameçon.

   f. L'adresse URL dans le courriel semble être une adresse « https:// », mais lorsqu'on clique dessus, on est dirigé vers une adresse « http:// ». Pourquoi est-ce un indice d'hameçonnage?
      - Éléments de réponse : Les sites Web sécurisés affichent une icône de cadenas fermé ou débutent par « https:// » et sont dignes de confiance. Lorsque l'adresse URL dirige l'utilisateur ou l'utilisatrice vers un site non sécurisé, c'est une tromperie.

Pour aller plus loin

- Campagne de sensibilisation
  a. Animer une discussion pour déterminer les stratégies que les élèves pourraient adopter pour sensibiliser l'ensemble des élèves de l'école aux tentatives d'hameçonnage.
  b. Demander aux élèves de mettre en place leur campagne de sensibilisation pour la classe, l'école ou la communauté (p. ex., affiches, vidéos, poèmes, annonces publicitaires).

Ne mordez pas à l'hameçon!



ACTIVITÉS SUGGÉRÉES

BILLET DE SORTIE

Ne mordez pas à l'hameçon! (Individuel)

Photocopier le **Billet de sortie : Ne mordez pas à l'hameçon!** (voir Annexe D) et le remettre à chaque élève. Demander aux élèves de répondre aux questions du billet de sortie.

Option « ère numérique »

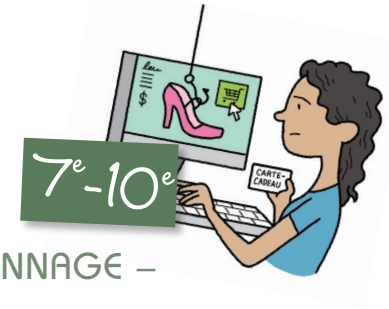
Créer une version numérique du **Billet de sortie : Ne mordez pas à l'hameçon!** et permettre aux élèves de le remplir en ligne.

RESSOURCES COMPLÉMENTAIRES

Jeux-questionnaires iCN : Transactions numériques 7-10, Identité numérique 7-10

Écoles branchées : Qu'est-ce que l'identité numérique? (pages 6 et 7)
Conseils aux parents : Comment assurer la sécurité en ligne de votre enfant (pages 24, 25, 26 et 27)

Ne mordez pas à l'hameçon!

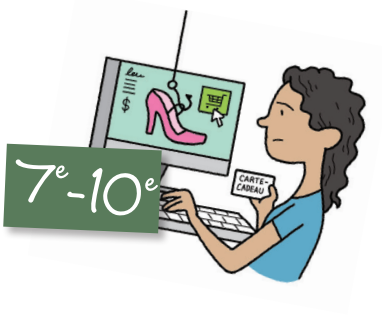


ANNEXE A – ACTIVITÉ DE REMUE-MÉNINGES : INDICES D'HAMEÇONNAGE – ÉLÉMENTS DE RÉPONSE

Voici quelques critères que les élèves pourraient dégager lorsqu'on leur demande d'indiquer des indices qui pourraient leur permettre de reconnaître un courriel hameçon.

INDICE	EXPLICATION
Nom	Le courriel est adressé de façon très vague « à qui de droit » ou « cher client » et ne contient pas le nom de la personne qui reçoit le courriel.
Nom de l'auteur ou de l'auteure du courriel, adresse courriel	Le nom de l'auteur ou de l'auteure du courriel est souvent vague. L'adresse courriel est souvent trompeuse afin de masquer le véritable compte utilisé pour effectuer l'envoi.
Coordonnées	Le message ne comporte aucune coordonnée qui permettrait de communiquer avec un représentant ou une représentante; aucun nom et aucun numéro de téléphone ne sont présents.
Logo	Le message contient souvent un logo qui correspond à celui d'une compagnie ou d'une entreprise connue. L'intention est de tromper même si ces logos sont facilement accessibles en ligne.
Faux hyperlien, adresse URL du site Web	Le courriel présente un faux hyperlien qui mène souvent à un site Web frauduleux où les gens qui se laissent prendre à l'hameçon peuvent entrer leurs renseignements qui seront envoyés aux gens malhonnêtes qui cherchent à usurper leur identité. Bien que le lien visible indique souvent une adresse sécurisée qui débute par « https:// », lorsqu'on clique sur le lien, le site Web qui s'ouvre est souvent un site non sécurisé dont l'adresse débute par « http:// ».
Date de publication, date de mise à jour	Il n'y a aucune date de publication ou la date affichée n'est pas récente. S'il n'y a pas de date de publication, il n'est pas facile de déterminer si l'information présentée sur le site Web est encore valide.
Fautes d'orthographe, majuscules mal placées	Le courriel comporte de nombreuses fautes d'orthographe ou des majuscules mal placées. C'est un indice que le contenu du courriel n'a pas été révisé avant d'être envoyé, ce qui est rare lorsqu'un courriel provient véritablement d'une source fiable.
Délai, urgence	Le sujet du courriel suggère souvent que l'information est sensible au facteur temps (p. ex., urgent, attention). Le courriel indique souvent un délai très court pour entrer ou mettre à jour ses renseignements personnels. L'intention est que le sentiment d'empressement fera en sorte que la destinatrice ou le destinataire du courriel ne prendra pas la peine de vérifier attentivement sa provenance, faute de temps.
Menace	Le courriel présente souvent la menace d'une conséquence grave qui risque de ne pas plaire à la destinatrice ou au destinataire du courriel. La conséquence aura lieu à moins que les renseignements voulus soient entrés sur le site Web indiqué dans le courriel.

Ne mordez pas à l'hameçon!

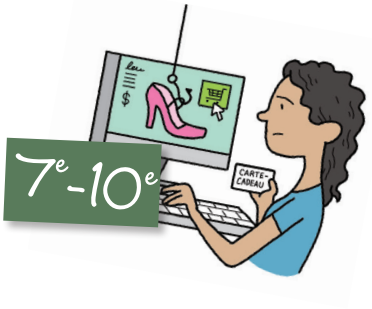


ANNEXE B – FICHE D'ANALYSE D'UN COURRIEL HAMEÇON

Étudie l'exemple de courriel hameçon (voir Annexe C) et note, dans le tableau ci-dessous, les indices qui peuvent t'aider à déterminer que c'est un courriel hameçon.

INDICE D'HAMEÇONNAGE	PREUVE À L'APPUI
Indice 1 :	
Indice 2 :	
Indice 3 :	
Indice 4 :	
Indice 5 :	
Indice 6 :	
Indice 7 :	

Ne mordez pas à l'hameçon!



ANNEXE C – EXEMPLE DE COURRIEL HAMEÇON

Urgent : Confirmation requise

Marchand 123 (service@mrchand123.com)

Toi (toi@courriel.com)

Urgent : Confirmation requise

Marchand 123

Cher client/chère cliente :

Merci d'avoir effectué un Achat chez Marchand 123. Notre section de sécurité a signalé que vous devez confirmer votre information Bancaire avant que nous procédions à la livraison de votre marchandise. Veuillez confirmer vos infos au site Web suivant :

https://www.marchand123.com/confirmation

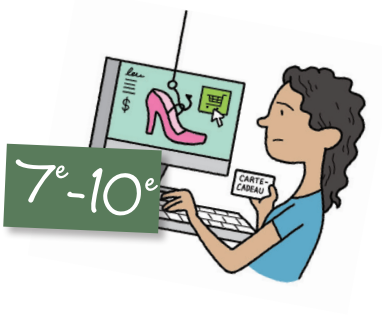
Accéder au lien :http://192.198.777.255.com/confirmation

Notez bien : Si votre compte n'est pas vérifié dans un Délai de 48 heures, votre achat sera annulé et aucun remboursement ne sera émis.

Merci.

Département de sécurité
Marchand 123

Ne mordez pas à l'hameçon!



ANNEXE D – BILLET DE SORTIE : NE MORDEZ PAS À L'HAMEÇON!

Nom : _____

Groupe : _____

Date : _____

1. Quels sont les objectifs de l'hameçonnage?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. Indique trois indices qui pourraient t'aider à déceler un courriel hameçon.

1._____

2._____

3._____

3. Décris trois mesures à prendre pour protéger tes renseignements personnels si tu crois être victime d'hameçonnage.

1._____

2._____

3._____