

Ressource pour le programme d'études

Cybersécurité : partie 2

Alignement avec le CLAO

Compétence	Groupe de tâches	Niveau
Compétence D — Utiliser la technologie numérique	s. o.	1
Compétence A — Rechercher et utiliser de l'information	A1. Lire des textes continus	1
Choisir un élément.	Choisir un élément.	Choisir un élément.
Choisir un élément.	Choisir un élément.	Choisir un élément.
Choisir un élément.	Choisir un élément.	Choisir un élément.

Voies de transition (cochez toutes les cases qui s'appliquent)

- | | |
|---|---|
| <input type="checkbox"/> Emploi | <input type="checkbox"/> Études postsecondaires |
| <input type="checkbox"/> Formation en apprentissage | <input checked="" type="checkbox"/> Autonomie |
| <input type="checkbox"/> Études secondaires | |

Compétences pour réussir intégrées (cochez toutes les cases qui s'appliquent)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Adaptabilité | <input type="checkbox"/> Calcul |
| <input type="checkbox"/> Collaboration | <input checked="" type="checkbox"/> Résolution de problème |
| <input checked="" type="checkbox"/> Communication | <input checked="" type="checkbox"/> Lecture |
| <input type="checkbox"/> Créativité et innovation | <input type="checkbox"/> Rédaction |
| <input checked="" type="checkbox"/> Compétences numériques | |

Notes : Ce document peut être consulté en complément de la ressource *Cybersécurité : partie 1* ou comme second volet.

Cybersécurité : partie 2

Qu'est-ce que la cybersécurité?

Les ordinateurs et les téléphones intelligents sont utiles dans la société moderne, et ils peuvent être très divertissants. Toutefois, leur utilisation comporte des risques. La cybersécurité consiste à gérer ces risques.

La cybersécurité consiste à se protéger contre les risques liés à l'utilisation d'un ordinateur ou d'un téléphone intelligent.



Objectifs de cette ressource

Cette ressource présente une introduction aux éléments ci-après :

- ✓ comment se protéger contre le **HAMEÇONNAGE** et d'autres arnaques;
- ✓ comment se protéger des **cyberprédateurs** et des **cyberprédatrices**, ainsi que du **vol d'identité** en ligne;
- ✓ comment effectuer des achats en ligne en toute sécurité;
- ✓ comment éviter la **cyberintimidation**;



En plus de :

- ✓ quelques activités pratiques pour vous assurer que vous êtes sur la bonne voie.

Table des matières

Qu'est-ce que la cybersécurité?	1
Objectifs de cette ressource	1
1. Introduction : à quoi sert la cybersécurité?	3
Quels sont les risques?	3
2. Hameçonnage	4
Comment cela se produit-il?	4
Que pouvez-vous faire?	5
Activité 1	7
3. Autres arnaques	9
4. Cyberintimidation	11
Quels sont les risques?	11
Que pouvez-vous faire?	13
5. Cyberprédateurs et cyberprédatrices	14
Quels sont les risques?	15
Que pouvez-vous faire?	15
6. Faites des achats en ligne en toute sécurité	17
Quels sont les risques?	17
Que pouvez-vous faire?	17
Activité 2	20
7. Survol	21
Réponses à l'activité 1	21
Réponses à l'activité 2	23



1. Introduction : à quoi sert la cybersécurité?

Il n'y a pas lieu d'avoir peur d'utiliser un ordinateur, un téléphone intelligent, une tablette ou Internet. Il convient toutefois de faire preuve de **vigilance** et de **prudence** afin d'éviter les risques réels.

Quels sont les risques?

- Si vous communiquez vos renseignements à de mauvaises personnes, vous pourriez devenir la cible d'**HAMEÇONNAGE** et d'un vol d'identité.
- Si vous ne faites pas preuve de discernement lorsque vous recevez des courriels ou des textos, vous pourriez devenir la cible d'autres **arnaques** en ligne.
- Si vous utilisez les médias sociaux, vous pourriez faire face à la **cyberintimidation**.
- Si vous ne faites pas attention aux personnes avec lesquelles vous interagissez en ligne, vous pourriez devenir la cible d'un **cyberprédateur** ou d'une **cyberprédatrice**.
- Si vous ne faites pas vos achats avec discernement, vous pourriez être la cible d'**arnaques en ligne**.



2. Hameçonnage

Le terme « **hameçonnage** » désigne les astuces en ligne utilisées pour commettre un **vol d'identité**. On parle de vol d'identité lorsque quelqu'un **vole** suffisamment de renseignements à votre sujet afin de pouvoir se faire passer pour vous en ligne, ce qui entraîne de **nombreuses conséquences néfastes**.

Comment cela se produit-il?

La principale astuce consiste à envoyer un **texto** ou un **courriel** vous demandant des renseignements personnels. *Ces textos ou courriels peuvent solliciter votre :*

- nom d'utilisateur;
- mot de passe;
- numéro de carte de crédit;
- information bancaire;
- numéro d'assurance sociale;
- date de naissance.



Quels sont les risques?

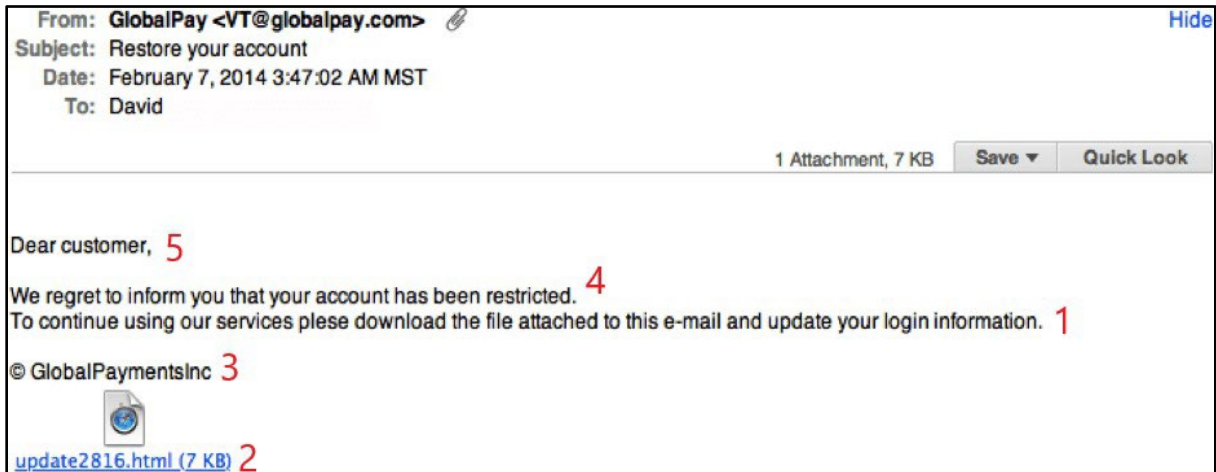
L'hameçonnage est la forme d'attaque en ligne la plus courante. Avec suffisamment de renseignements, une personne peut **voler votre identité** et :

- obtenir une nouvelle **carte de crédit en votre nom**, pour laquelle vous pourriez être responsable;
- accéder à votre compte bancaire et **voler votre argent**;
- effectuer des achats à partir de **votre compte bancaire** ou de **votre carte de crédit**;
- modifier vos mots de passe ou d'autres renseignements pour vous **empêcher d'accéder à vos propres comptes**.

Que pouvez-vous faire?

a. FAITES ATTENTION aux courriels frauduleux.

Les courriels frauduleux présentent souvent certaines caractéristiques dont il faut se méfier. Prenons l'exemple suivant :



N.B. Puisque ce genre de courriel est majoritairement envoyé en anglais, nous avons choisi de ne pas les traduire. Cependant, il faut s'en méfier qu'importe la langue utilisée!

1. Dans ces courriels, on vous **incite généralement à fournir des renseignements personnels**.
2. On vous invite à **cliquer sur un lien**.
3. Ces courriels revêtent souvent un caractère **officiel** et semblent provenir d'une institution bancaire, d'une entreprise ou d'un organisme gouvernemental.
4. Ces courriels contiennent souvent des **termes inquiétants** ou **urgents** comme « **Votre compte a été suspendu** » ou « **FAITES VITE** » ou « **RETARD** » ou « **DERNIÈRE CHANCE** » pour vous mettre sous pression.
5. Dans ces courriels, on **utilise rarement votre nom**, et on s'adresse à vous comme « Cher client » ou « Chère cliente. »
6. Vérifiez l'adresse électronique de l'expéditeur ou de l'expéditrice. Même si on utilise le nom d'une entreprise, l'adresse électronique est souvent manifestement fausse.



IMPORTANT : Ne vous laissez pas tromper par l'aspect officiel des courriels ou par les moyens de pression contenus dans le message!

Ne fournissez JAMAIS de renseignements confidentiels dans un courriel.

Le moyen le plus simple de vous protéger contre une attaque par hameçonnage est de **ne JAMAIS envoyer par courriel** des renseignements comme vos mots de passe, votre date de naissance, vos renseignements bancaires ou votre numéro d'assurance sociale.

IMPORTANT :

- ***Votre institution bancaire ne vous demandera JAMAIS de lui fournir des renseignements par courriel.***
 - ***Votre institution bancaire vous appellera toujours pour vous parler directement ou vous demandera de vous rendre dans une succursale.***
7. Ne cliquez **JAMAIS** sur des liens suspects contenus dans des courriels, même si on vous incite à le faire.
8. **EXAMINEZ** régulièrement vos renseignements bancaires et vos relevés de carte de crédit pour vous assurer qu'ils sont corrects et qu'il n'y a pas de charges que vous ne reconnaissez pas.
- Si vous constatez une anomalie, appelez votre banque ou la société Émettrice de votre carte de crédit afin de procéder immédiatement à une annulation!*



Activité 1

Malgré le fait que ces exemples soient en anglais, pouvez-vous cibler les indices qui démontrent qu'il s'agit d'hameçonnage?

Voici trois différents courriels hameçons. Pour chacun, suivez les étapes ci-après :


- encerclez les indices** qui portent à croire qu'il s'agit d'un courriel hameçon;
- expliquez** ci-dessous pourquoi vous avez encerclé chaque indice;
- consultez** les réponses qui figurent à la fin de cette ressource.



Encerclez les indices d'hameçonnage et expliquez-les.

Courriel hameçon 1 :

There's issue with your American Express account




American Express <administraciones@pentagon-seguridad.cl>
To hashedout@thesslstore.com

↩ Reply
↩ Reply All
→ Forward
...

Fri 11/8/2019 5:29 AM

ⓘ This message was sent with High importance.
 If there are problems with how this message is displayed, click here to view it in a web browser.



Review Your Information.

Due to recent activities on your account, we placed a temporary suspension until you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

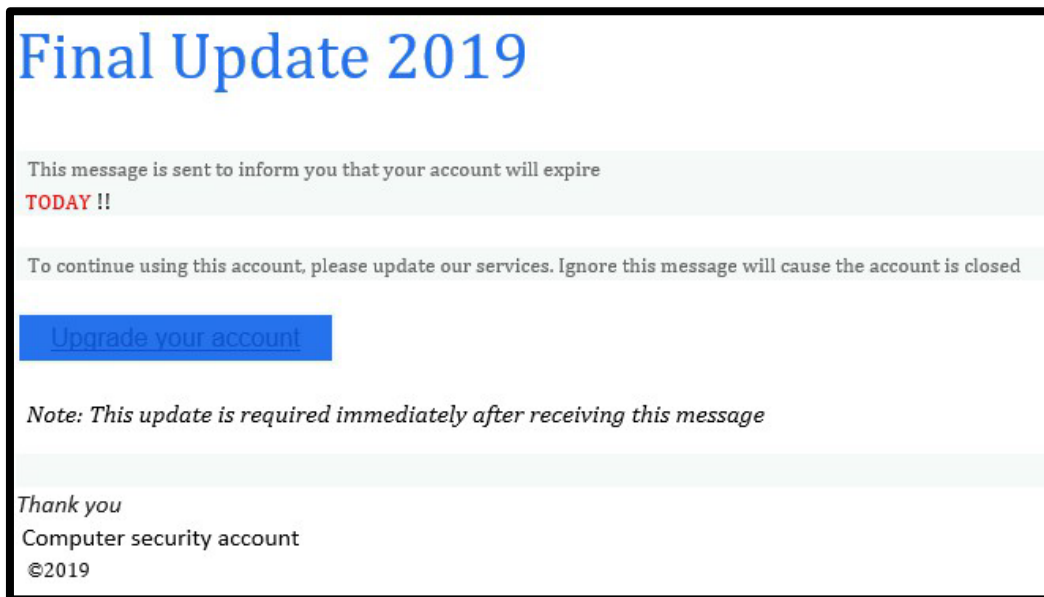
[Click here to review your account now](#)

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,
American Express Company. All rights reserved

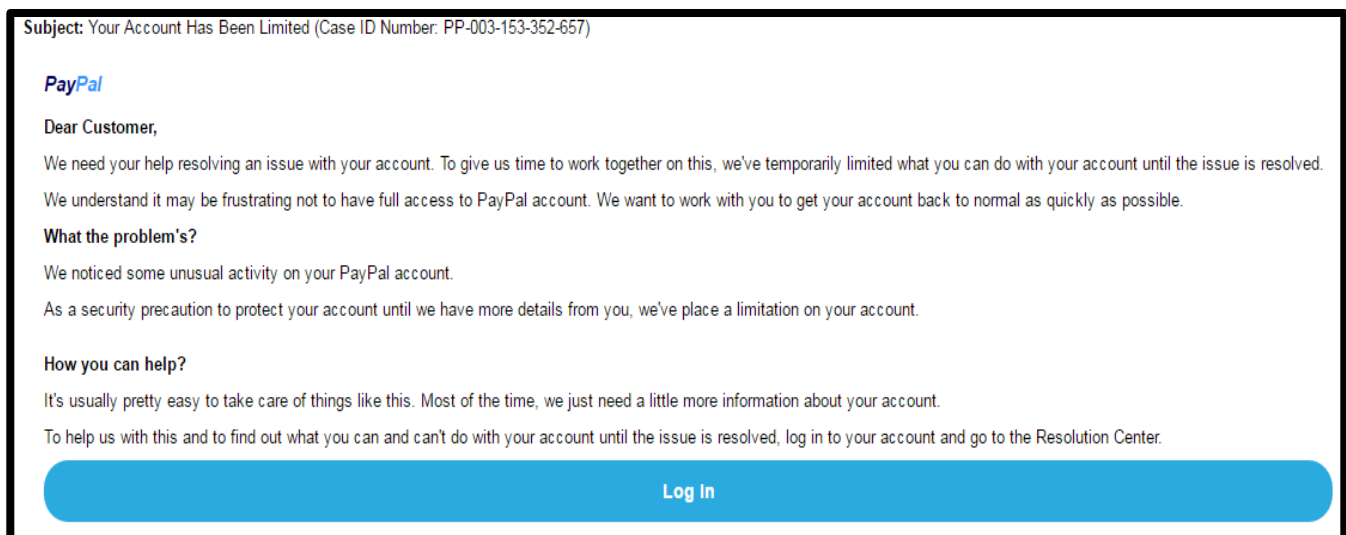
Encerclez les indices d'hameçonnage et expliquez-les.

Courriel hameçon 2 :



Encerclez les indices d'hameçonnage et expliquez-les.

Courriel hameçon 3 :



3. Autres arnaques

a. Arnaques de proposition de prix

Il arrive que des arnaqueurs essaient de vous attirer avec des courriels qui vous offrent une chance de **gagner rapidement de l'argent ou des prix**.

IMPORTANT:

- *Les entreprises véritables n'envoient pas de propositions de prix par courriel.*
- *Ne cliquez JAMAIS sur un tel lien, même si on vous offre un prix!*



N.B. Puisque ce genre de courriel est majoritairement envoyé en anglais, nous avons choisi de ne pas les traduire. Cependant, il faut s'en méfier!

b. Arnaques relatives aux cartes de crédit préapprouvées

Si vous avez besoin d'argent, il peut être tentant de recevoir un courriel vous informant que vous êtes « **préapprouvée** » pour une carte de crédit. Parfois, ces offres vous demandent de **payer des frais avant de recevoir** votre carte de crédit.



IMPORTANT:

- *Les vraies sociétés de cartes de crédit n'envoient JAMAIS une offre préapprouvée par courriel.*
- *Les vraies sociétés de cartes de crédit ne demandent JAMAIS de payer des frais d'avance.*

c. *Arnaques relatives aux programmes basés sur la peur (« Scareware » en anglais)*

Il peut arriver que votre ordinateur affiche une fenêtre contextuelle vous avertissant que votre ordinateur est infecté par un **virus**. On vous demandera de cliquer sur un lien pour **télécharger un logiciel « antivirus. »**

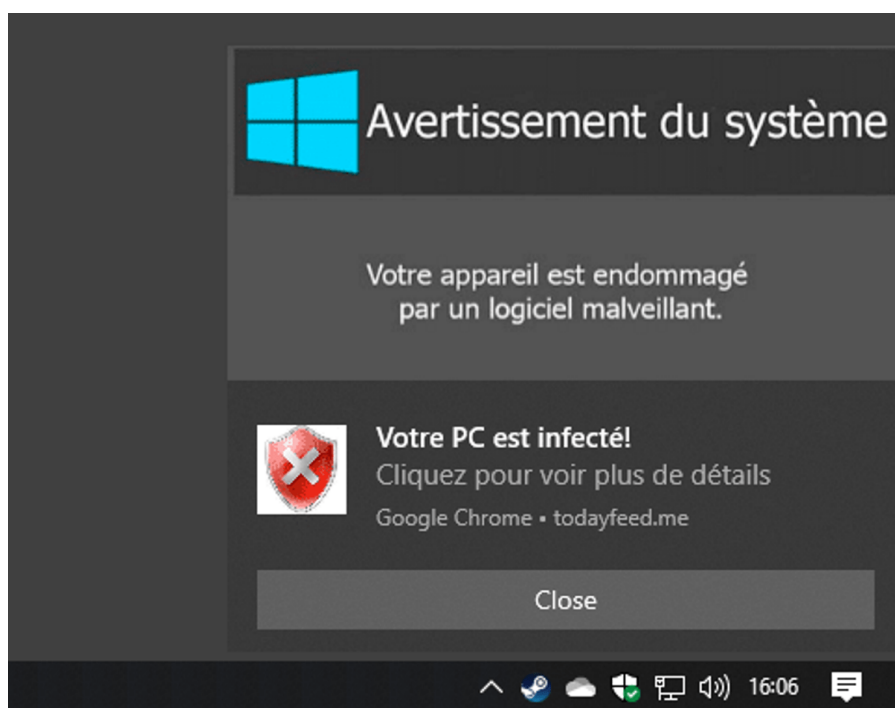


Image tirée de : alexbacher.fr

La fenêtre contextuelle signale la présence d'un virus, mais ce n'est qu'en cliquant dessus que vous obtiendrez réellement un virus sur votre ordinateur.

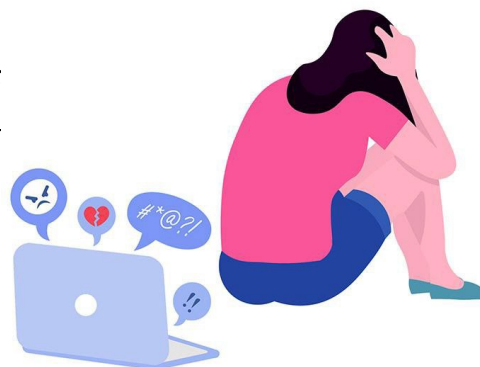
Si vous cliquez sur la fenêtre contextuelle, vous risquez d’être redirigé ou redirigée vers une nouvelle page où l’on vous demandera les numéros de votre carte de crédit pour payer le faux logiciel « antivirus. » Pour **éviter** cela, faites ce qui suit :

- ne cliquez **JAMAIS** sur une telle fenêtre depuis votre appareil électronique;
- utilisez le logiciel antivirus **gratuit** qui est déjà installé sur votre appareil électronique;
- procurez-vous un logiciel **antivirus de meilleure qualité** directement sur un site Web réputé comme [Norton Antivirus](#) ou [McAfee Antivirus](#).

4. Cyberintimidation

Tout comme dans le monde réel, Internet peut être un lieu où **de vieilles connaissances se retrouvent** et où **de nouvelles amitiés se forment**. Mais, plus encore que dans le monde réel, Internet peut être un lieu où les gens **se voient maltraités**.

*La **cyberintimidation** consiste à traiter les autres avec méchanceté ou cruauté en ligne. Ce phénomène est surtout répandu chez les adolescents et les adolescentes, mais elle peut aussi toucher les adultes.*



Quels sont les risques?

La cyberintimidation se produit presque toujours dans les médias sociaux comme Facebook, Twitter, TikTok, Snapchat et Instagram. *Elle peut se manifester sous de **nombreuses formes** et avoir de **multiples conséquences**.*

a. Formes de cyberintimidation

Harcèlement

- Publier des messages **désobligeants** à l’égard de quelqu’un.
- **Perturber** quelqu’un avec des messages, des questions ou des insultes.
- Publier des commérages ou d’autres renseignements mesquins à propos de quelqu’un pour **nuire à sa réputation**.



Exclusion

- Expulser quelqu'un d'un groupe de médias sociaux comme un groupe de discussion ou un groupe Facebook.

Révélation

- Rvéler les renseignements personnels ou les secrets d'une personne dans un forum en ligne.
- Publier en ligne des photos révélatrices ou embarrassantes de quelqu'un.



Cyberharcèlement

- Harcèlement répété d'une personne en ligne. Recherche de renseignements privés ou de l'emplacement d'une personne.



La cyberintimidation peut être pire que l'intimidation dans la vie réelle.

b. Conséquences de la cyberintimidation

La cyberintimidation peut avoir de graves conséquences pour ses victimes :

- sentiments de dévalorisation, de stress et de solitude;
- menaces sur l'emploi ou la vie scolaire de la victime;
- **dépression et pensées suicidaires;**
- *les messages peuvent demeurer **en ligne à jamais** et être accessibles à n'importe qui dans le monde entier.*

Que pouvez-vous faire?

La cyberintimidation peut être une expérience dévastatrice, mais il existe des moyens de la **prévenir** et d'y **faire face**.

a. *Racontez aux autres ce qui vous arrive.*

- Ne vous sentez pas obligé de traverser cette épreuve seul ou seule.
- Parlez-en à vos amis et amies et à vos proches, puis **demandez conseil**.
- En cas de menaces ou de discours haineux, **signalez les actes d'intimidation à la police**.





Certains actes d'intimidation sont illégaux et peuvent être sanctionnés par la loi.

b. *Bloquez les personnes qui vous harcèlent.*


c. *Signalez la cyberintimidation à la plateforme de médias sociaux à l'aide de ses outils de signalement.*

Le moyen le plus simple de ne plus recevoir de messages de harcèlement est de bloquer la personne qui les envoie.

Pour retirer un ami ou une amie de Facebook :

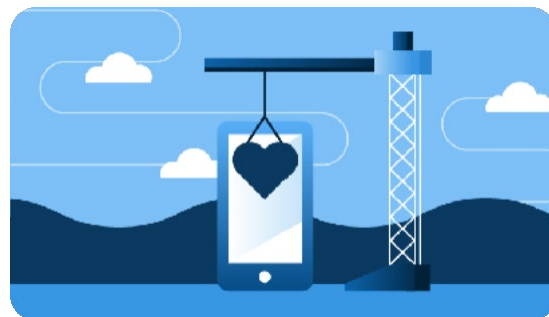
1. Tapez son nom dans la barre de recherche en haut de la page Facebook.
2. Cliquez sur l'icône  **Ami(e)s** dans le haut de son profil.
3. Cliquez sur l'icône  **Retirer des ami(e)s**.

***Pour empêcher quelqu'un de vous envoyer des textos :***

1. Appuyez sur le nom ou le numéro de la personne en haut.
2. Appuyez sur l'icône , faites défiler vers le bas, puis appuyez sur « **Bloquer ce correspondant.** »

Utilisez correctement les médias sociaux.

- Prenez une pause des médias sociaux de temps en temps.
- Soyez calme et poli ou polie dans vos échanges en ligne.
- ***Ne faites pas vous-même de l'intimidation!***

**5. Cyberprédateurs et cyberprédatrices**

Il est rare que de très mauvaises personnes en ligne veuillent plus que voler votre argent ou votre identité. Les pires cyberprédateurs et cyberprédatrices sont **dangereux** et **dangereuses**, et il convient de les prendre très au sérieux et de les éviter à tout prix.



Quels sont les risques?

Les cyberprédateurs et cyberprédatrices **prétendent toujours être quelqu'un qu'ils ou qu'elles ne sont pas** — c'est ce qu'on appelle les « **ARNAQUEURS** » et les « **ARNAQUEUSES.** » Ils ou elles essaient de vous faire croire qu'ils sont quelqu'un d'autre pour vous entraîner dans une relation afin de vous faire du **mal** d'une manière ou d'une autre.

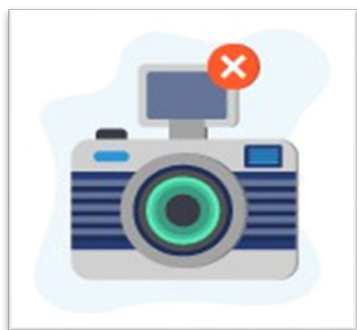
IMPORTANT :

Leurs motivations vont du vol à la VIOLENCE.

Que pouvez-vous faire?

Pour éviter les cyberprédateurs et les cyberprédatrices, il faut savoir repérer les personnes qui se font passer pour quelqu'un d'autre, ou les « arnaqueurs » et les « arnaqueuses. »

Le meilleur moyen de repérer une personne qui tente d'arnaquer est en se posant les questions suivantes.



- A) Est-elle d'accord avec tout ce que vous dites?
- B) En sait-elle déjà beaucoup sur vous?
- C) Est-elle plus séduisante que d'habitude et a-t-elle une photo qui semble professionnelle?

Si cette personne est particulièrement gentille ou attirante, cela pourrait être « trop beau pour être vrai. »



- ☐ A-t-elle un profil très récent et peu d'amis ou d'amies?
- ☐ Évite-t-elle les appels en face à face?

Si elle ne laisse pas beaucoup de traces en ligne et ne montre pas son visage, il s'agit d'un indicateur d'alerte.



Si elle ne laisse pas beaucoup de traces en ligne et ne montre pas son visage, il s'agit d'un indicateur d'alerte.

- ☐ Vous demande-t-elle de l'argent ou des images explicites?
- ☐ Veut-elle vous rencontrer en personne?

Ce sont là les principaux indicateurs d'alerte.



IMPORTANT :

Ne donnez JAMAIS d'argent ou d'images de vous à quelqu'un que vous avez rencontré en ligne.

Ne rencontrez JAMAIS quelqu'un en personne si vous n'avez la certitude absolue que cela ne présente aucun danger.

Même si vous avez la certitude que cela ne présente aucun danger, ne rencontrez quelqu'un en personne que dans un endroit sûr où il y a d'autres personnes, comme un café ou même une bibliothèque. Ne rencontrez jamais quelqu'un seul ou seule!

6. Faites des achats en ligne en toute sécurité

Faire des achats en ligne peut être pratique. Vous pouvez acheter des articles qui ne sont pas vendus dans les magasins locaux et les faire livrer directement chez vous.

Mais, il existe des **arnaques liées au magasinage en ligne** qui peuvent vous coûter beaucoup d'**argent** et vous occasionner beaucoup de **peine**. Il est donc important de connaître les risques et de savoir comment y faire face.



Quels sont les risques?

- Le principal risque lié aux achats en ligne est de **payer pour quelque chose que vous n'obtiendrez jamais**.*
- Vous pourriez aussi communiquer vos **numéros de votre carte de crédit** à des personnes peu dignes de confiance.*
- Une personne pourrait se connecter à votre compte d'achat et **acheter des choses pour elle-même**.*
- En tant que vendeur ou vendeuse, vous pourriez expédier un article sans **jamais recevoir de paiement**.*

Que pouvez-vous faire?

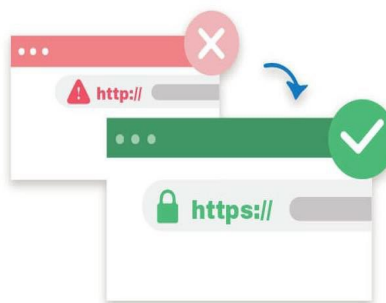
N'utilisez que des sites Web de confiance.

- Les sites Web d'entreprises de confiance sont les plus surs.
- Ces entreprises ont des sites Web sécurisés, mais vous devriez toujours effectuer vos vérifications.



Vous saurez que le site Web que vous utilisez est sécurisé de deux manières différentes, c'est-à-dire au moyen de :

- l'icône de verrouillage à la fin de la barre d'adresse;
- la lettre « s », qui figure dans l'adresse du site Web sécurisé (<https://>), alors que les sites Web non sécurisés ne contiennent pas la lettre « s, » qui signifie **SÉCURISÉ**.



Utilisez des **mots de passe robustes** pour vos comptes d'achat en ligne. Évitez d'effectuer vos achats sur des **ordinateurs publics**, mais, si vous le faites, veillez à vous déconnecter lorsque vous avez terminé afin que la prochaine personne utilisant l'ordinateur ne puisse pas accéder à vos renseignements.

- Si vous oubliez de vous déconnecter, des personnes pourraient **acheter des articles sur votre compte** et modifier les renseignements qui y figurent.



Vérifiez régulièrement vos relevés de cartes de crédit.

- Si vous constatez une transaction inhabituelle ou suspecte, appelez votre institution bancaire ou rendez-lui visite immédiatement et annulez vos cartes de crédit.



Lisez les avis!

- Il est conseillé de lire les avis sur l'article que vous envisagez d'acheter, **surtout** si vous ne pouvez pas le voir et le toucher.



Si vous faites un achat sur un forum de vente de seconde main comme Kijiji ou Facebook Marketplace, vous devriez toujours lire les avis des vendeurs et des vendeuses pour savoir si vous pouvez leur faire **confiance**.

Quelques derniers indicateurs d'alerte concernant les achats en ligne

- Utilisez-vous un mode de paiement **SÉCURISÉ**, comme une carte de crédit, ou un mode de paiement **NON SÉCURISÉ**, comme un virement bancaire?
- Vous sentez-vous **pressé** ou **pressée**?
- L'offre semble-t-elle « **trop bonne pour être vraie?** » *Si oui, c'est sans doute le cas!*
- *Ne donnez jamais votre numéro de téléphone et ne répondez jamais à une personne qui vous demande d'obtenir un code pour elle. Il s'agit d'une arnaque courante sur Facebook Marketplace. Bloquez immédiatement ce compte.*

Activité 2

Encerclez autant d'indices que possible qui montrent que cette expérience d'achat n'est **pas sûre** :

canadian-benefit.gov@outlook.com Subj: 100001
Government Of Canada sent you \$540.00 (CAD) and the money is waiting to be deposited into your bank account.

Message:
Government Of Canada has started to sending out federal payment by e-Transfer. Click here to deposit your funds: federal-redirect.com

Reference number: CA2vSg6e

Data rates may apply

Expliquez vos raisons et consultez les réponses à la fin du document:

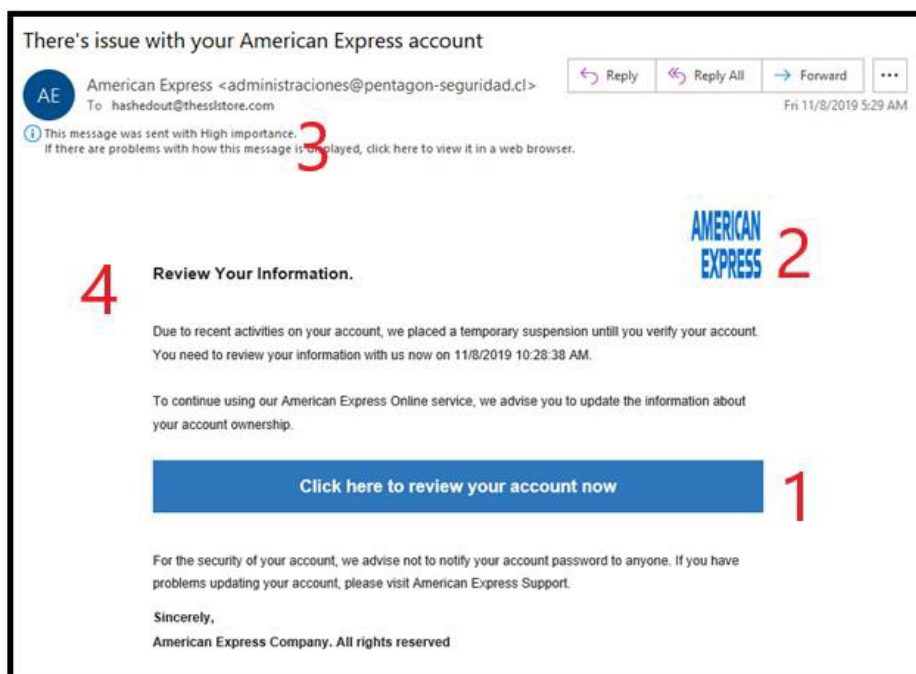
7. Survol

*Vous connaissez maintenant les **risques** liés à l'utilisation d'un ordinateur, d'un téléphone intelligent ou des médias sociaux.*

- Vous avez appris à vous protéger contre les attaques d'**HAMEÇONNAGE** et d'autres arnaques.
- Vous avez appris à éviter la **cyberintimidation** et les **cyberprédateurs** et **cyberprédatrices**, ainsi qu'à y faire face.
- Vous avez également appris à **faire des achats en ligne en toute sécurité**.
- Vous pouvez vous référer à ce guide à tout moment pour revoir les étapes à suivre pour utiliser Facebook.

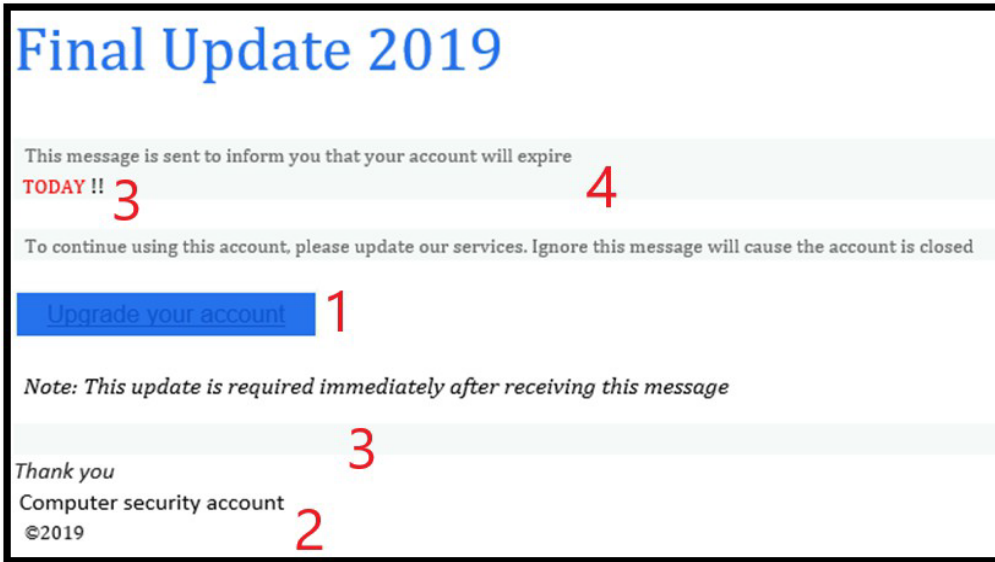
Réponses à l'activité 1

1.



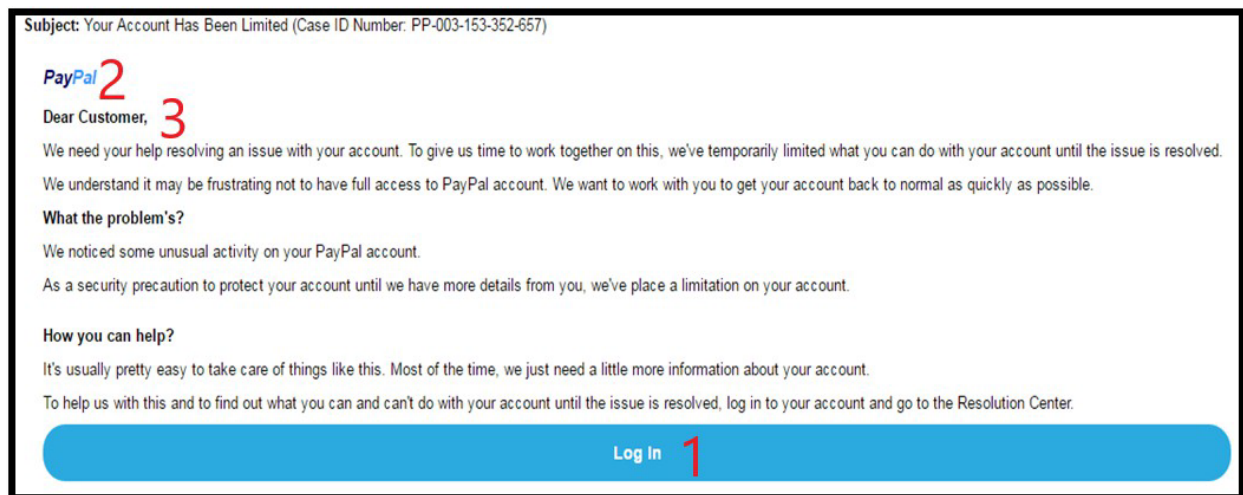
1. On me demande de cliquer sur un lien.
2. Le message semble officiel.
3. Le message contient des mots pressants.
4. Mon vrai nom n'y est pas.

2.



1. On me demande de cliquer sur un lien.
2. Le message semble officiel.
3. Le message contient des mots pressants.
4. Mon vrai nom n'y est pas.

3.



1. On me demande de cliquer sur un lien.
2. Le message semble officiel.
3. Mon vrai nom n'y est pas.

Réponses à l'activité 2



canadian-benefit.gov@outlook.com Subj: 100001
Government Of Canada sent you \$540.00 (CAD) and the money is waiting to be deposited into your bank account.

Message:
Government Of Canada has started to sending out federal payment by e-Transfer. Click here to deposit your funds: federal-redirect.com

Reference number: CA2vSg6e

Data rates may apply

1. Il ne s'agit pas d'un site Web sécurisé.
2. On essaie de vous presser.
3. L'offre est « trop bonne pour être vraie. »
4. Le mode de paiement proposé n'est pas sûr.

* Cette activité est tirée du site Web ci-après : <https://antifraudcentre-centreantifraude.ca/scams-fraudes/phishing-hameconnage-fra.htm#a2>