Question d'argent

pour les personnes ayant des aptitudes différentes

Cahier 6
Sécurité de l'argent

Alpha pour la vie Canada

Commanditaire principal

LA PROMESSE TD
PRÊTS À AGIR

Question d'argent

Bienvenue à *Question d'argent*!

Question d'argent a été conçu pour vous aider à bien prendre soin de vous, en vous permettant de bien prendre soin de votre argent.

Lorsque vous vous sentez bien par rapport à votre gestion financière, vous êtes moins stressé et vous avez plus de temps et d'énergie à consacrer aux choses qui vous tiennent à cœur.

Qu'allez-vous apprendre?

Dans le module d'aujourd'hui, l'apprentissage portera sur :

- **La sécurité en ligne**
- **Les fraudes par hameçonnage**
- **Le vol d'identité**
- **L'exploitation financière**

ABC
Alpha pour la vie Canada

Qu'est-ce que la sécurité de l'argent?

La sécurité de l'argent signifie tout ce que vous pouvez faire pour protéger votre argent et vos informations personnelles.

Activité

Penser à la sécurité de l'argent

Voici quelques personnes qui expliquent ci-dessous la façon dont elles utilisent leur argent et leurs informations personnelles. Pensez-vous que ces façons sont sûres ou dangereuses? Entourez votre réponse.

« Je ne transporte que l'**argent** dont j'ai besoin. »	**Sûr**	**Dangereux**	**Je ne sais pas**
« J'utilise un code **NIP** facile à deviner, au cas où je l'oublierais. »	**Sûr**	**Dangereux**	**Je ne sais pas**
« J'utilise l'ordinateur public de la bibliothèque pour mes **services bancaires en ligne**. »	**Sûr**	**Dangereux**	**Je ne sais pas**

L'argent comptant c'est du papier-monnaie et des pièces de monnaie.

Le **NIP** est l'abréviation de « numéro d'identification personnel ». Votre NIP est votre mot de passe pour utiliser votre carte de débit.

Les services bancaires en ligne, c'est lorsque vous utilisez un ordinateur pour effectuer vos opérations bancaires sur Internet.

Une **carte de débit** est une carte bancaire qui vous permet de dépenser de l'argent de votre compte bancaire.

« J'utilise le smartphone de mon voisin pour mes **services bancaires mobiles**. »	**Sûr**	**Dangereux**	**Je ne sais pas**
« Lorsque je m'inquiète pour la sécurité de mon argent, je parle à une personne de confiance. »	**Sûr**	**Dangereux**	**Je ne sais pas**

Les services bancaires mobiles consistent à utiliser une tablette ou un smartphone pour effectuer vos opérations bancaires.

Discussion de groupe

Des personnes dans votre groupe ont-elles entouré des réponses différentes aux vôtres? Quelles sont leurs raisons?

Protéger votre argent et vos informations personnelles

Voici quelques conseils qui pourraient vous aider à protéger votre argent et vos informations personnelles.

Ne transportez que l'argent dont vous avez besoin
Si vous transportez beaucoup d'**argent comptant**, vous risquez de le perdre ou qu'on le vole.

Utilisez des mots de passe et des codes NIP difficiles à deviner
Si votre mot de passe ou code **NIP** est trop simple, des personnes malhonnêtes pourraient le deviner. Si quelqu'un d'autre peut deviner votre mot de passe ou votre **NIP**, il peut voler votre argent et vos informations personnelles.

Utilisez un ordinateur privé (comme un ordinateur à la maison, si vous en avez un) pour les services bancaires en ligne
Les personnes malhonnêtes peuvent voler des informations sur les ordinateurs publics.

D'autres conseils pour vous aider à protéger votre argent et vos informations personnelles se trouvent à la page suivante!

Voici quelques conseils supplémentaires qui pourraient vous aider à protéger votre argent et vos informations personnelles.

Utilisez une connexion Internet privée (comme votre connexion Internet à la maison, si vous en avez) pour les services bancaires en ligne et mobiles
Les personnes malhonnêtes peuvent voler des informations sur les connexions Internet publiques.

Utilisez uniquement votre smartphone personnel ou celui d'une personne de confiance pour les services bancaires mobiles
Les smartphones enregistrent parfois vos informations. Si une personne malhonnête utilise le même smartphone, elle peut voler vos informations.

Parlez à quelqu'un de confiance si vous n'êtes pas sûr
Parfois, il est difficile de dire si quelque chose est sûre ou dangereuse. Essayez de parler de la sécurité financière à une personne de confiance ou à un employé de la banque.

Pourquoi la sécurité de l'argent est-elle importante?

La sécurité de l'argent veut dire protéger votre argent et votre **identité**. Si votre argent et votre **identité** ne sont pas en sécurité, des personnes malhonnêtes pourraient vous les voler.

Dans le reste de cette cahier, nous allons en apprendre davantage sur la protection de votre argent et de votre **identité**.

Protéger votre identité

Il est très important de protéger votre **identité**. Vos informations personnelles sont privées et vous ne devez les partager qu'avec des personnes de confiance.

Si des personnes malhonnêtes volent vos informations personnelles, elles peuvent se faire passer pour vous. Il s'agit d'un crime appelé l**e vol d'identité**.

Votre **identité** est l'ensemble de vos informations personnelles. Votre identité peut inclure :

- Votre nom complet
- Votre date de naissance
- Votre numéro d'assurance sociale (NAS)
- Tous vos mots de passe

Le vol d'identité est une sorte de crime où des personnes malhonnêtes volent les informations personnelles de quelqu'un et se font passer pour cette personne.

En qui avez-vous confiance?

Quelles sont les personnes en qui vous avez confiance en matière de vos informations personnelles? Voici une liste de personnes en qui vous pourriez avoir confiance.

N'oubliez pas que tout le monde fait confiance à des personnes différentes. Vous n'êtes pas obligé de faire confiance à toutes les personnes sur cette liste.

- Vos parents
- Vos frères et sœurs
- Vos enfants
- Les employés de banque
- Les employés du gouvernement
- Votre meilleur ami

Y a-t-il quelqu'un d'autre à qui vous pouvez confier vos informations personnelles?

Le saviez-vous?

Vous avez le droit de protéger votre argent et vos informations personnelles. Personne n'est autorisé à prendre votre argent ou vos informations personnelles sans votre permission.

Services bancaires en ligne et mobile

La **banque en ligne** c'est quand vous utilisez un ordinateur pour effectuer vos opérations bancaires sur Internet. La **banque mobile** c'est quand vous utilisez un smartphone ou une tablette pour effectuer vos opérations bancaires.

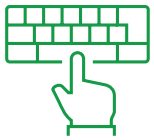
Voici ce que vous pouvez faire avec les services bancaires **en ligne** et **mobiles** :

- Vérifiez l'activité et le solde de votre compte bancaire
- Payez vos factures en ligne
- Transférez de l'argent entre vos comptes bancaires
- Envoyez de l'argent à d'autres personnes par **virement électronique**

Un **virement électronique** signifie envoyer de l'argent à une personne par Internet à l'aide d'un ordinateur, d'une tablette ou d'un smartphone.

Différentes banques vous permettent de faire différentes choses avec les **services bancaires en ligne**, comme ouvrir un nouveau compte ou payer vos factures. Vous pouvez visiter ou appeler votre banque pour apprendre plus sur leurs **services bancaires en ligne** et **mobiles**.

Activité



Créer un mot de passe fort

Il est important de créer un mot de passe fort lorsque vous vous inscrivez aux **services bancaires en ligne** et **mobiles**. Un mot de passe faible est facile à deviner par quelqu'un d'autre, mais un mot de passe fort ne l'est pas.

Un mot de passe fort a un mélange de :

- chiffres **2 67 91**
- lettres minuscules **c g k**
- lettres majuscules **F Z H**
- symboles **! $ # ?**

Voici quelques exemples de mots de passe. Pensez-vous que ces mots de passe sont forts ou faibles?

abc123	**Fort**	**Faible**	**Je ne sais pas**
odCD7c#21	**Fort**	**Faible**	**Je ne sais pas**
password	**Fort**	**Faible**	**Je ne sais pas**
1111111	**Fort**	**Faible**	**Je ne sais pas**
83!feS3%	**Fort**	**Faible**	**Je ne sais pas**
E35!?fri3O	**Fort**	**Faible**	**Je ne sais pas**

Sécurité bancaire en ligne et mobile

Voici d'autres moyens de protéger votre compte bancaire en ligne :

- Utilisez uniquement le site Web ou l'application officiel de votre banque pour les s**ervices bancaires en ligne** ou **mobiles**
- Ne communiquez à personne votre nom d'utilisateur ou votre mot de passe pour les **services bancaires en ligne** ou **mobiles**
- Évitez d'utiliser des ordinateurs publics ou des connexions Internet publiques pour effectuer vos opérations **bancaires en ligne** ou **mobiles**.
- Demandez à un employé de la banque s'il existe d'autres moyens de protéger votre compte bancaire.

Nous vous présentons Ali

Ali fait des efforts pour protéger son **identité** :

- Il utilise des mots de passe forts et difficiles à deviner
- Il déchire des papiers contenant des informations personnelles avant de les recycler
- Il ne partage des informations personnelles qu'avec ses parents, les employés de banque et les fonctionnaires du gouvernement

Discussion de groupe

Utilisez-vous les mêmes conseils qu'Ali pour protéger votre **identité**? Que pouvez-vous faire d'autre pour protéger votre **identité**?

Notes:

L'histoire d'Ali

Ali vient de commencer à utiliser les **services bancaires en ligne**. Il est heureux, car maintenant c'est facile de voir combien d'argent il a. Il aime aussi payer ses factures en ligne.

Un jour, Ali reçoit un courriel qui dit :

LB

De : Banque locale <local-bank@gr564.com>
Object : Action requise - Information incomplète
Date : Jeu 2020-02-13 12:56 AM
À : Ali

< >>

Cher client,

Cet courriel vise à vous informer que votre porfil de services bancaires en ligne avec la Banque locale est incomplet. Cliquez sur le lien ci-dessous et entrez votre mot de passe bancaire pour compléter votre profil.

http://info.localbank.ca/completeprofile

Cordialement,

LOCAL BANK

« Ce courriel semble sérieux », dit Ali. « Je me demande si je devrais leur donner mon mot de passe? »

Discussion de groupe

Pensez-vous que Ali peut partager son mot de passe bancaire en toute sécurité? Pourquoi ou pourquoi pas?

Hameçonnage

Le courriel d'Ali est une sorte de **fraude** appelée **hameçonnage**.

Une **fraude** est un projet illégal pour tromper les gens et les voler.

Le **hameçonnage** est une fraude qui utilise des courriels, des appels téléphoniques ou des message texte. Les fraudes par hameçonnage tentent de vous voler des informations personnelles. Elles prétendent généralement provenir de quelqu'un ou d'un endroit en qui vous avez confiance, comme un membre de votre famille ou votre banque.

Voici quelques indices indiquant qu'un courriel est du **hameçonnage**. Pouvez-vous trouver ces indices dans le courriel d'Ali?

1.

À : Ali

Cher client,

Cet courriel vise à vous informer que

Parfois, les courriels de hameçonnage n'utilisent pas votre nom. Ces courriels peuvent utiliser un mot différent, tel que «Client».

2.

vous informer que votre porfil de services ba
ue locale est incomplet. Cliquez sur le lien ci
t de passe bancaire pour compléter votre prc

Les courriels de **hameçonnage** contiennent souvent des erreurs, comme des mots mal orthographiés. Un courriel professionnel ne contient probablement pas d'erreurs.

3.

ligne avec la Banque locale est incomplet. Cliquez su
et entrez votre mot de passe bancaire pour compléter

Les courriels de **hameçonnage** vous demandent généralement des informations personnelles. Les banques ne demandent pas vos informations personnelles dans des courriels ou des message texte. Vous ne devez jamais divulguer d'informations personnelles en ligne ou par message texte.

4. et entrez votre mot de passe bancaire pour compléter http://info.localbank.ca/completeprofile

Les courriels de **hameçonnage** peuvent vous envoyer vers un site Web où ils voleront vos informations personnelles. Parfois, le site Web dit **http://**. Habituellement, les sites Web officiels indiquent **https://** au lieu de **http://**. Le « **s** » supplémentaire signifie « **sécurisé** ».

5. Cordialement,

LOCAL BANK

Les courriels de **hameçonnage** essaient de donner l'impression qu'ils proviennent réellement de votre banque ou d'une autre source fiable. Même si un courriel a le bon logo ou si son adresse courriel semble correcte, il peut toujours s'agir d'un courriel de hameçonnage.

Voici quelques indices supplémentaires qu'un courriel pourrait être une **fraude** par **hameçonnage** :

- Le courriel vous avertit d'une activité suspecte sur votre compte
- Le courriel indique qu'il y a un problème avec votre compte
- Le courriel indique que vous avez droit à un remboursement fiscal ou à des choses gratuites
- Le courriel indique que le problème est urgent et que vous devez réagir rapidement

Ali pense avoir reçu un courriel de **hameçonnage**. Il téléphone à sa banque et l'employé de la banque lui dit que la Banque locale n'a pas envoyé ce courriel.

Ali supprime le courriel de **hameçonnage**.

Les informations personnelles d'Ali sont en sécurité!

Fraudes par hameçonnage: que faire

Voici ce que vous devez faire si vous pensez qu'un courriel est une **fraude** par **hameçonnage** :

- **Si vous recevez un courriel et que vous pensez qu'il s'agit d'une fraude, ne partagez aucune information!**
- **Faites une recherche en ligne du numéro de téléphone de l'organisme. Contactez le et demandez s'il vous a envoyé un courriel.**
- **N'ouvrez aucune pièce jointe et ne cliquez sur aucun lien dans le courriel**
- **Ne répondez pas au courriel**
- **Marquez le courriel comme étant un pourriel**
- **Supprimer le courriel**

Conseil

Parfois, les **fraudes** par **hameçonnage** sont des message texte ou des appels téléphoniques. Un message texte ou un appel téléphonique peut être du **hameçonnage** si :

- s'il provient de quelqu'un que vous ne connaissez pas
- vous n'attendiez pas l'appel ou le message texte

Si vous pensez qu'un appel ou un message texte constitue du **hameçonnage**, ne partagez aucune information!

Entraînons-nous

Voici un autre courriel de **hameçonnage**. Pouvez-vous repérer des indices qui indiquent que ce courriel est une **fraude**?

Avec un partenaire ou tout (e) seul (e), essayez d'entourer quelques indices indiquant que ce courriel est une **fraude** par **hameçonnage**.

CR

De : Agence du revenu du Canada <tax-refund@can.gov.agancy.com>
Object : Remboursement d'impôt
Date : Ven 2020-02-28 15:15 PM
À : Contribuable

< >>

Agence du revenu du Canada
Canada
Agence du revenu du Canada

Cher contribuable,

Après avoir examiné vos formulaires fiscaux de 2018, nous avons déterminé que vous avez droit à un remboursement d'impôt de 362,58 $. Pour demander votre remboursement, remplissez le formulaire sur le site Web de l'Agence du revenu du Canada: http://canada-rev-agency.com.

Cordialement,

Agence du revenu du Canada

Discussion de groupe

Des personnes dans votre groupe ont-il trouvé des indices différents? Pourquoi ont-ils choisi ces indices?

Vol d'identité : que faire

Même lorsque nous faisons des efforts pour protéger nos informations, les gens trouvent parfois un moyen de les voler. Voici la marche à suivre si vous pensez que quelqu'un a volé vos informations personnelles.

Qu'est-ce-qu'ils ont volé?	Que devriez-vous faire?
Vos informations bancaires, **carte de crédit** ou **carte de débit**	**Contactez votre banque.** Vous pouvez y aller en personne ou appeler le numéro de téléphone sur votre dernier relevé bancaire ou de **carte de crédit**. Un employé de banque vous dira quoi faire ensuite.
Vos autres informations personnelles	**Contactez la police et votre banque.** Dites à la police et à votre banque que vous souhaitez signaler un **vol d'identité**. Vous pouvez le faire en y aller en personne ou par téléphone. Ils vous diront quoi faire ensuite.

Une **carte de crédit** est une carte qui vous permet d'acheter maintenant et de payer plus tard.

Autres moyens de protéger votre identité

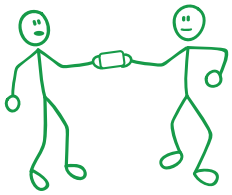
- Déchirez des papiers contenant vos informations personnelles avant de les jeter
- Utilisez des mots de passe difficiles à deviner et ne les écrivez pas
- Ne partagez pas votre numéro d'assurance sociale avec des personnes en qui vous ne faites pas confiance
- Refusez si les gens vous demandent de dépenser de l'argent ou de partager des informations qui vous mettent mal à l'aise.
- Vous pouvez toujours parler à quelqu'un en qui vous avez confiance avant de prendre de grandes décisions.

Exploitation financière

Il y a abus financier lorsque quelqu'un en qui vous avez confiance utilise votre argent, vos biens ou votre **identité** sans votre permission.

C'est de l'exploitation financière

L'ami d'Ali, Cathy, a utilisé la **carte de crédit** d'Ali pour acheter des vêtements. Cathy n'est pas autorisée à utiliser la **carte de crédit** d'Ali, mais elle l'a quand même utilisée. Ali ne sait pas si Cathy le remboursera.



Ce n'est pas de l'exploitation financière

Le frère d'Ali, Mohammed, demande l'autorisation d'emprunter la **carte de crédit** d'Ali. Ali accepte et Mohammed le rembourse tout de suite.

Signes de l'exploitation financière

Parfois, il peut être difficile de dire s'il y a abus financier. Ces questions peuvent vous aider à comprendre si vous subissez une exploitation financière.

Entourez la réponse dans la case qui vous semble vraie.

Est-ce que quelqu'un d'autre utilise votre argent sans votre permission?	**Oui**	**Non**	**Je ne sais pas**
Si quelqu'un d'autre prend des décisions concernant votre argent, cache-t-il des informations ou vous ment-il concernant votre argent?	**Oui**	**Non**	**Je ne sais pas**
Votre argent ou d'autres effets personnels disparaissent-ils?	**Oui**	**Non**	**Je ne sais pas**
Avez-vous l'impression que quelqu'un essaie de vous éloigner des personnes que vous connaissez?	**Oui**	**Non**	**Je ne sais pas**
Quelqu'un d'autre dissimule-t-il votre argent, même s'il n'est pas censé le faire?	**Oui**	**Non**	**Je ne sais pas**

Avez-vous répondu « Oui » ou « Je ne sais pas » à des questions?

Vous êtes peut-être victime d'une exploitation financière. La page suivante vous indique quoi faire.

Avez-vous répondu « non » à chaque question?

C'est génial! Rappelez-vous de protéger votre argent et vos informations personnelles.

Exploitation financière: quoi faire

Pensez-vous que vous subissez une exploitation financière? Pensez-vous que quelqu'un que vous connaissez subit une exploitation financière?

Voici ce qu'il faut faire.

Il est important de dire à quelqu'un que vous pensez être victime d'une exploitation financière. Parlez à quelqu'un en qui vous avez confiance, par exemple :

- un membre de la famille
- un ami proche
- un employé de votre banque
- votre médecin

Si vous sentez que vous êtes en danger immédiat, appelez la police et demandez de l'aide.

Voulez-vous vous assurer que vous êtes à l'abri des abus financiers? Voici quelques actions que vous pouvez effectuer :

- **Assurez le suivi de votre argent**
  Prenez des notes de tout l'argent que vous dépensez ou donnez pour vous aider à conserver une trace de votre argent.
- **Demandez de l'aide pour les décisions importantes**
  Demandez à une personne de confiance d'examiner les contrats ou autres accords importants avant de les signer.
- **Restez en contact avec votre famille et vos amis**
  Il est important d'avoir plusieurs personnes à qui parler et qui peuvent vous aider.

Sécurité de l'argent

Ce que nous avons appris aujourd'hui

Aujourd'hui, nous avons appris :

- La sécurité en ligne
- Les fraudes par hameçonnage
- Le vol d'identité
- L'exploitation financière

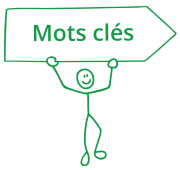
Rappel

Vous avez le droit de protéger votre argent et vos informations personnelles. Personne n'est autorisé à prendre votre argent ou vos informations personnelles sans votre permission.

Entraînez-vous

Pensez à quelque chose que vous pouvez faire aujourd'hui pour sécuriser votre argent et vos informations personnelles. Vous pouvez peut-être suivre vos dépenses ou renforcer votre mot de passe des **services bancaires en ligne**. Si vous savez ce que vous voulez faire, écrivez-le ici.

Je vais sécuriser mon argent et mes informations personnelles en :



Argent comptant	Le papier-monnaie et les pièces de monnaie
Carte de crédit	Une carte qui vous permet d'acheter maintenant et de payer plus tard
Carte de débit	Une carte bancaire qui vous permet de dépenser de l'argent de votre compte bancaire
Fraude	Un plan illégal pour tromper les gens et les voler
Hameçonnage	Le hameçonnage est une fraude qui utilise des courriels, des appels téléphoniques ou des messages textes. Les fraudes par hameçonnage tentent de vous voler des informations personnelles. Elles prétendent généralement provenir de quelqu'un ou d'un endroit en qui vous avez confiance, comme un membre de votre famille ou votre banque.
Identité	Ce sont toutes vos informations personnelles. Votre identité peut inclure : • Votre nom au complet • Votre date de naissance • Votre numéro d'assurance sociale (NAS) • Tous vos mots de passe

NIP	C'est l'abréviation de « numéro d'identification personnel ». Votre NIP est votre mot de passe pour utiliser votre carte de débit
Service bancaire en ligne	C'est l'utilisation d'un ordinateur pour effectuer vos opérations bancaires sur Internet
Service bancaire mobile	C'est l'utilisation d'une tablette ou d'un smartphone pour effectuer vos opérations bancaires
Virement électronique	C'est l'envoi d'argent à quelqu'un sur Internet à l'aide d'un ordinateur, d'une tablette ou d'un smartphone
Vol d'identité	Un type de crime où des personnes malhonnêtes volent les informations personnelles de quelqu'un et se font passer pour elle

Plus d'informations

Le gouvernement du Canada a un « Petit livre noir de la **fraude** » qui vous explique comment repérer les **fraudes** et comment y faire face.
https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04333.html

La Banque TD a plus d'informations sur les fraudes en ligne, y compris des conseils pour protéger votre ordinateur et comment prévenir les fraudes.
https://www.td.com/francais/confidentialite-et-securite/confidentialite-et-securite/comment-vous-proteger-vous-meme/protect-yourself.jsp

ABC Alpha pour la vie Canada a des ressources en ligne pour vous aider à en savoir plus sur la gestion financière.
https://questiondargent.ca/ressources/

Merci de votre participation à *Question d'argent pour les personnes ayant des aptitudes différentes*!

ABC Alpha pour la vie Canada

Commanditaire principal

TD LA PROMESSE TD PRÊTS À AGIR