7e à 12e année

La vie privée en ligne : les codes d'accès

Adaptation française : Centre franco-ontarien de ressources pédagogiques

ROGERS cybersecure catalyst

Les codes d'accès, plus souvent appelés mots de passe, sont essentiels pour protéger les renseignements personnels et privés. On entend par renseignements personnels les faits sur une personne (ses passe-temps, ses aliments préférés, etc.), tandis que les renseignements privés, comme son adresse, son numéro de téléphone ou sa date de naissance, peuvent servir à l'identifier. Entre les mains de la mauvaise personne, ces deux types de renseignements peuvent servir à deviner ou à « déchiffrer » les mots de passe, et à accéder à des comptes en ligne, comme ceux de services bancaires en ligne et de courriels. Par exemple, si tu as fait une publication sur ta célébrité ou ton athlète préféré et que tu utilises le nom de cette personne dans un mot de passe, ce dernier sera facile à deviner. Un mot de passe peut être composé d'une série de mots aléatoires, d'une phrase facile à retenir ou d'une combinaison de mots, de chiffres et de symboles; quel qu'il soit, il doit être unique à toi. C'est comme une empreinte digitale!

Les mots de passe sont nécessaires pour ta sécurité, et pour protéger ta vie privée. Des mots de passe forts et différents pour chaque compte empêchent les autres d'accéder à tes comptes et à tes appareils en se faisant passer pour toi. Il faut y faire attention et ne jamais les divulguer. Autrement, tu risques de perdre tes comptes, d'entacher ta réputation, ou de te faire voler ton identité.

Dans cette ressource, tu apprendras comment créer un mot de passe sûr et facile à retenir, comment protéger tes mots de passe, comment les attaques sont menées, et comment gérer tes mots de passe.

Créer des mots de passe forts

Les mots de passe protègent ta vie privée et empêchent les autres d'accéder à tes comptes et à tes renseignements privés. C'est important, car les gens ne pourront pas prétendre être toi, fouiller dans tes affaires, te voler, entacher ton image en ligne, ou même t'attirer des ennuis. Pour cette raison, il est important de suivre quelques règles simples sur les mots de passe pour qu'ils soient sûrs et impossibles à deviner :

- **La longueur fait la force! Les longs mots de passe sont plus difficiles à deviner, et à déchiffrer pour les pirates. La plupart des comptes exigent un mot de passe d'au moins 10 caractères; toutefois, la longueur recommandée est de 12 à 15 caractères.**

- **Utilise une phrase de passe! Une phrase de passe peut être composée de mots aléatoires qui sont faciles à retenir.**

- **N'utilise jamais de renseignements personnels ou privés dans ton mot de passe ou ta phrase de passe – des renseignements possiblement déjà connus des autres ou faciles à obtenir – car les voleuses et voleurs d'identité peuvent s'en servir pour se faire passer pour toi.**

- **Si ton mot de passe contient des chiffres (fortement recommandé!), ne répète pas le même chiffre, comme « 777 », et n'utilise pas de séries de comme « 123 » ni de date importante comme « 010101 », si ta fête est le 1er janvier 2001. C'est trop facile à deviner!**

- **Crée des mots de passe avec divers types de caractères! Cela inclut les majuscules (A, B, C), les minuscules (a, b, c), les chiffres (1, 2, 3) et les symboles (!, @, #). L'utilisation de ces quatre types de caractères renforce le mot de passe.**

Caractères
Les caractères d'un mot de passe sont les symboles qui sont constitués de lettres majuscules et minuscules, de chiffres allant de 0 à 9, et de caractères comme !, #, ^, *, $, %.

Phrase de passe

Les phrases de passe contiennent souvent plus de caractères que les mots de passe, mais moins de composantes (par exemple, quatre mots au lieu de 12 caractères aléatoires).

Procédés mnémotechniques

Se prononce « mnemotɛknik »; il s'agit d'une technique (schémas de lettres, d'idées ou d'associations) qui facilite la mémorisation.

Créer un mot de passe fort : conseils utiles

Tu as de la difficulté à trouver des mots de passe forts et sécuritaires? Essaie ces conseils pratiques :

- **Tu peux utiliser une technique de mémorisation ou d'apprentissage comme le procédé mnémotechnique pour créer et retenir des mots de passe forts. Par exemple, la citation « Sois toi-même, il n'y a pas mieux. » – Taylor Swift, 2016 devient : Stm,inapm-TS,2016.**

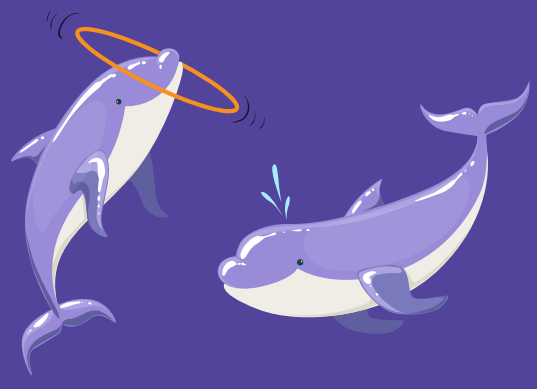
- **Combine les langues! Par exemple, la phrase de passe « Le chat mange trois bijoux! » en anglais, en espagnol, en italien et en français devient : The,Gato,Mangia,3BIJOUX!**

- **Fais un poète de toi! Essaie de créer un mot de passe ou une phrase de passe avec des allitérations ou des rimes! Exemple : « Des.dauphins.délicats.dansent. doucement! »**

Allitération
Répétition de la même lettre ou du même son au début de mots adjacents ou près les uns des autres.

À ne pas oublier!

Lorsque tu crées une phrase de passe, choisis des mots que tu peux visualiser afin de les retenir facilement. Par exemple : DesDauphinsDélicatsDansent



B PERTINENCE

Protection des mots de passe

Créer un mot de passe fort est primordial, mais il ne sera utile que si tu le protèges et le gardes pour toi! Voici comment te protéger et protéger ton mot de passe :

- **Ne donne ton mot de passe à *personne***, même pas à une amie ou un ami afin de poursuivre une série de parties en ligne ou pour prouver ton amitié!
- Assure-toi de **dire à tes parents ou tutrices et tuteurs où sont consignés tes mots de passe**, en cas d'urgence.
- **Ne permets pas à des sites Web, navigateurs et programmes de « se rappeler » de tes mots de passe ou de les « enregistrer »**, puisqu'ils peuvent facilement être compromis en cas d'infraction.
- **Ne te connecte pas à tes comptes sur les appareils des autres**, puisque tes mots de passe pourront facilement être récupérés. Si toutefois c'est nécessaire, assure-toi de te déconnecter lorsque tu as terminé.
- **Tape tes mots de passe loin des regards curieux**, surtout si tu te connectes à proximité de groupes, comme à la bibliothèque ou en classe.

- **Ne te connecte jamais à tes comptes lorsque tu utilises un réseau Wi-Fi public ou un réseau privé virtuel (VPN) gratuit**, puisque tous les renseignements sur les utilisateurs et sur leurs mots de passe peuvent être récupérés.

- **Ne consigne jamais tes mots de passe sur ton appareil.** Envisage plutôt d'utiliser un gestionnaire de mots de passe!

- **N'utilise aucun renseignement permettant de t'identifier** dans des noms d'utilisateur (nom, genre, emplacement, date d'anniversaire). Par exemple : MademoiselleLilly2002.

Gestionnaire de mots de passe
Programme informatique qui permet de consigner, de générer et de gérer les mots de passe pour des services en ligne. Il permet aussi de générer et de récupérer des mots de passe forts.

- **Traite les questions secrètes comme des mots de passe!** Choisis des questions et crée des réponses qui ne révèlent pas tes vrais renseignements personnels, puisqu'ils peuvent facilement être devinés par quelqu'un qui te connaît ou qui te suit potentiellement sur les médias sociaux.

- **Évite de jouer à des jeux ou de répondre à des questionnaires qui te demandent des renseignements personnels ou privés, ou qui te demandent de lier ton compte**, comme Facebook. Ces jeux sont une forme d'hameçonnage pour des renseignements qui pourraient t'amener à révéler ton mot de passe sans le savoir.

- **Déconnecte-toi de tes comptes et verrouille tes appareils** lorsque tu ne les utilises pas, afin que personne d'autre n'y ait accès.

Hameçonnage
Tentative frauduleuse ou fraude d'une usagère ou d'un usager d'Internet visant à obtenir des renseignements privés ou personnels à des fins illégales.

Qu'as-tu appris?

Selon toi, pourquoi est-ce que les gens se sentiraient obligés de divulguer leurs mots de passe? Quels sont les risques de donner ses mots de passe à d'autres?

Pirate informatique
Personne qui utilise la technologie pour accéder sans autorisation à des renseignements ou à des données.

Déchiffrer le code : comment les attaques sont menées

Tu peux avoir l'impression de ne pas avoir assez d'importance, de n'avoir rien à cacher ou à voler, ou te moquer que ton compte soit pris d'assaut. La réalité, c'est que les pirates utilisent des robots de recherche pour parcourir le Web à la recherche de vulnérabilités ou de brèches de sécurité – et ils ne sont pas sélectifs. Tu dois te soucier de ton identité personnelle, puisque quelqu'un peut prétendre être toi et te causer de nombreux soucis en publiant du contenu inapproprié sur tes comptes, en demandant de l'aide ou de l'argent à tes amies et amis ou à ta famille, ou en te bloquant l'accès à tous tes comptes.

Tes comptes peuvent devenir vulnérables au piratage et aux attaques de deux façons :

1. **Tes comptes deviennent vulnérables aux attaques par supposition de mots de passe lorsque tu choisis des mots de passe faibles.**
2. **Lorsque tes comptes sont compromis lors d'une atteinte à la protection des données, tes comptes et tes renseignements personnels deviennent vulnérables.**

Atteinte à la protection des données
Incident où un compte ou une base de données est piraté, et dont les noms d'utilisateurs, les mots de passe et les autres renseignements confidentiels consignés sont révélés.

Jetons un œil à trois attaques fréquentes par supposition de mots de passe :

- **Attaques par dictionnaire :** Ce type d'attaque utilise des dictionnaires informatisés de toutes les langues pour deviner un mot de passe, mais aussi des listes de mots de passe piratés et des chaînes de mots provenant de titres de livres, de slogans, de paroles de chansons, d'articles de journaux, etc.

- **Attaques par force brute :** Tous les mots de passe peuvent éventuellement être déchiffrés avec une attaque par force brute, mais le temps que cela prendra dépend de la force de ton mot de passe. Les mots de passe faibles peuvent être devinés en moins d'une minute, tandis que les mots de passe forts peuvent prendre des années ou des décennies à déchiffrer.

- **Attaques ciblées :** Les pirates peuvent dénicher beaucoup de renseignements sur les gens en ligne, et savent que certains de ces renseignements personnels peuvent être utilisés dans les mots de passe. Il est facile pour les pirates d'accéder à ces renseignements, même si elles et ils ne connaissent pas la victime personnellement.

Le savais-tu?

Un expert en sécurité qui voulait montrer aux gens que leurs données avaient été compromises a créé un site Web où l'on peut taper en toute sécurité notre courriel pour savoir s'il a été compromis.

Essaie-le!

Tape le site Web suivant (en anglais seulement) dans la barre d'adresse de ton navigateur : https://haveibeenpwned.com/

Si ton courriel a été compromis, déroule la page, et tu trouveras des détails quant à l'endroit où il a été piraté.

C APPEL À L'ACTION

La balle est dans ton camp! Gérer tes mots de passe

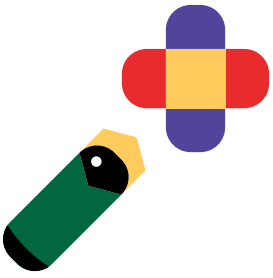
Maintenant que tu sais comment créer un mot de passe fort, le protéger, et que tu connais les types d'attaques de données, il est important de savoir comment gérer tes mots de passe – tous autant qu'ils sont!

- **N'utilise jamais le même mot de passe, ou les mêmes questions et réponses de sécurité**, pour plus d'un compte. Pourquoi pas? Car si l'un de tes comptes est piraté, les autres comptes utilisant le même nom d'utilisatrice ou d'utilisateur, courriel ou mot de passe ne seront pas aussi faciles à pirater!

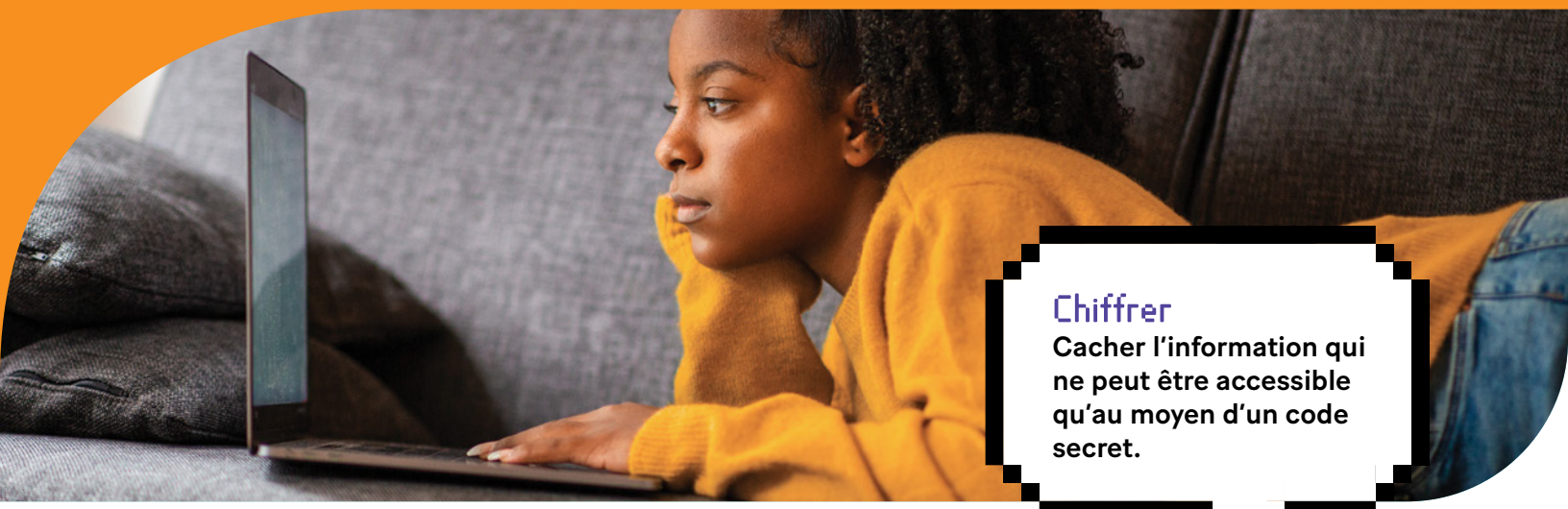
- **Change occasionnellement tes mots de passe.** Tu as peur d'oublier de le faire? Pourquoi ne pas prévoir une date à ton calendrier?

- **Ne réutilise pas de vieux mots de passe!**

- **Consigne tes mots de passe hors ligne et ailleurs que sur tes appareils.** Envisage d'utiliser un outil sécurisé de gestion des mots de passe (plus d'information ci-dessous) pour générer et consigner des mots de passe complexes pour chacun de tes comptes. **Utilise l'authentification à facteurs multiples (AFM)** partout où tu le peux. C'est une couche supplémentaire de protection, puisqu'avant d'avoir accès au compte, tu dois d'abord confirmer à partir d'un autre appareil (par exemple ton téléphone) que tu essaies de te connecter. Si quelqu'un connaît le mot de passe, il n'aura pas accès au compte grâce à l'AFM, et tu seras informé de la tentative.



Authentification à facteurs multiples (AFM)
Mesure de sécurité qui vérifie l'identité de l'utilisateur en exigeant une ou deux preuves ou identifiants supplémentaires (« facteurs »), comme des codes numériques ou des réponses à des questions de sécurité uniques.



Gestionnaire de mots de passe

Essayer de retenir une grande quantité de noms d'utilisatrices ou d'utilisateurs, de mots de passe et de comptes peut conduire à un trop-plein. Les gestionnaires de mots de passe tentent de régler ce problème en chiffrant tous tes mots de passe et identifiants – pour y avoir accès, tu n'as qu'à créer et taper un seul mot de passe fort.

Voici certains critères à garder en tête lorsque vient le temps de choisir un logiciel de gestion de mots de passe. Détermine lesquels sont les plus importants pour toi, et choisis le logiciel qui y répond. Inscris-toi, et c'est parti!

- ✓ Facilité de récupération des comptes
- ✓ Changement des mots de passe
- ✓ Façon dont sont consignées et protégées les données
- ✓ Capacités de partage
- ✓ Compatibilité avec plusieurs plateformes et applications d'authentification à facteurs multiples
- ✓ Capacité d'organisation de l'ensemble des comptes
- ✓ Inclusion d'un accès d'urgence
- ✓ Surveillance du Web caché
- ✓ Soutien
- ✓ Coût total par année

La technologie n'est pas toujours néfaste, mais il faut développer les connaissances nécessaires pour naviguer sur le Web en toute sécurité. Tôt ou tard, toutes les combinaisons de mots de passe possibles peuvent être piratées. La question est : combien de temps cela prendra-t-il?

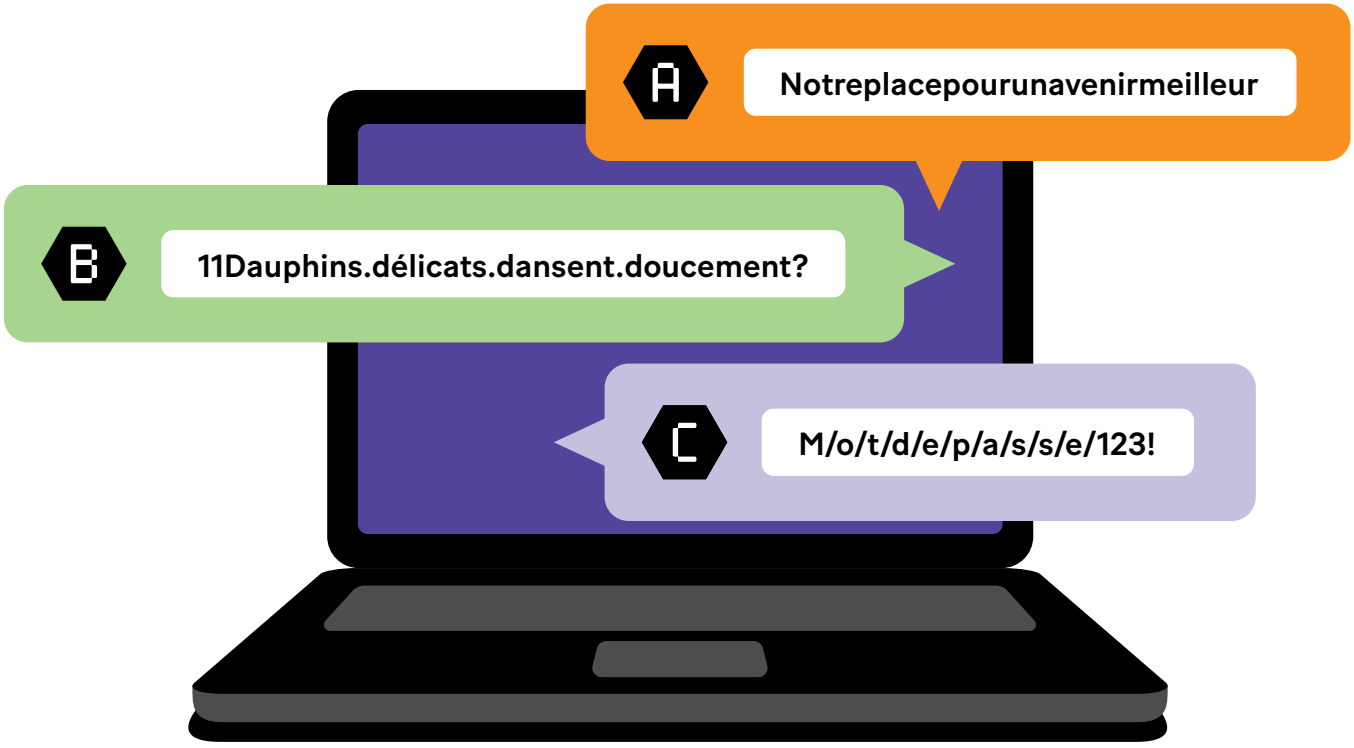
Activités

Les activités sont une bonne façon de t'exercer et de mettre en pratique tes connaissances sur le sujet abordé dans la ressource.

ACTIVITÉ 1

Classement des mots de passe

Classe les exemples de mots de passe ci-dessous du plus fort au plus faible, et explique ton raisonnement.



1 ..... POURQUOI? .....

2 ..... POURQUOI? .....

3 ..... POURQUOI? .....

Réponse :
1er : Mot de passe B (long, inhabituel, plusieurs chiffres et symboles)
2e : Mot de passe A (long, mais aucun symbole ni chiffre, les paroles de chansons sont plus faciles à deviner)
3e : Mot de passe C (trop courant, même s'il est séparé par des symboles)

ACTIVITÉ 2

Exercice de création de mots de passe

À l'aide des phrases ci-dessous ainsi que des conseils fournis dans cette ressource, essaie de créer tes propres exemples de mots de passe forts.

Phrase	Exemple de mot de passe
Trois mousquetaires	3M0usqueta1res! ✓
Ajoute-moi sur Instagram!	
« Que la force soit avec toi. » – La Guerre des étoiles (*Star Wars*), 1977	
« Je jure solennellement que mes intentions sont mauvaises. » – Harry Potter et le prisonnier d'Azkaban	

Tu veux mettre à l'épreuve la force des mots de passe que tu as créés? Essaie le vérificateur de mots de passe Kaspersky; il te dira à quel point ton mot de passe est résistant au piratage, et s'il est déjà apparu dans les bases de données de mots de passe divulgués.

Vérificateur de mots de passe Kaspersky*

https://password.kaspersky.com/fr/

*N.B. : Kaspersky ne recueille et ne consigne aucun mot de passe tapé sur le site Web.

POUR EN SAVOIR PLUS

Pour en savoir plus sur la cybersécurité ou pour poursuivre la conversation et l'apprentissage, consultez le site du Centre canadien pour la cybersécurité : cyber.gc.ca/fr/.

Pour en savoir plus sur les phrases de passe, les codes d'accès et les NIP, rendez-vous sur le site du gouvernement du Canada : pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/phrases-de-passe-mots-de-passe-et-nip.

Jeunesse, J'écoute

Pour de l'aide, envoyez un message texte au 686868 ou téléphonez au 1-800-668-6868 partout au Canada, 24 heures sur 24, 7 jours sur 7, ou accédez aux ressources en ligne sur jeunessejecoute.ca.

Toronto Metropolitan University

ROGERS cybersecure catalyst

Adaptation française : Centre franco-ontarien de ressources pédagogiques