4e à 6e année

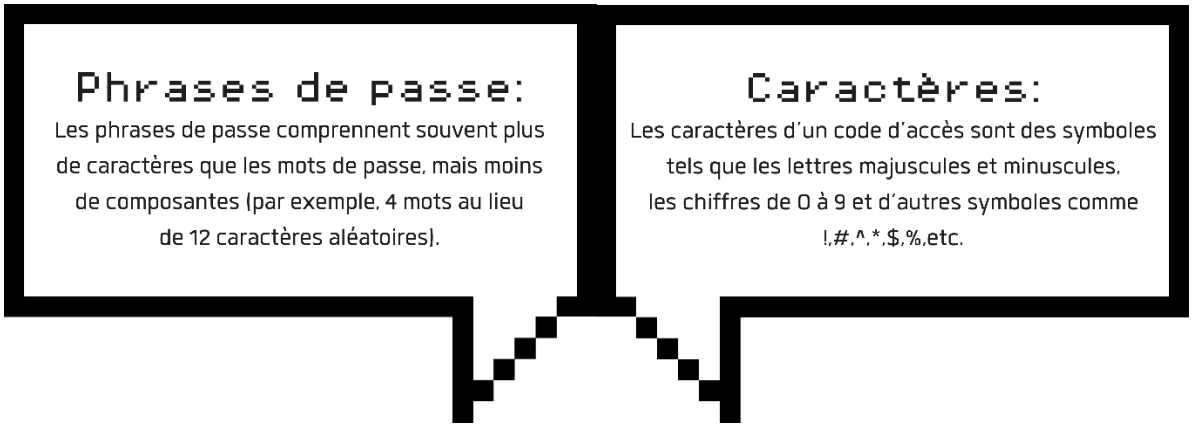
Cycle moyen (4e à 6e année) Documentation pour la leçon 4

Mots de passe et codes d'accès

Ryerson University
ROGERS cybersecure catalyst
Adaptation française : Centre franco-ontarien de ressources pédagogiques

Maintenant que tu as une empreinte numérique positive, comment fais-tu pour la protéger?

Créer des mots de passe forts :



Plus il est long, plus il est fort! Les codes d'accès longs sont plus difficiles à deviner pour les autres. La plupart des comptes en ligne requièrent des codes d'accès 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 constituée d'une suite de quelques mots aléatoires faciles à mémoriser. Si tu as besoin d'aide pour en trouver une, essaie d'utiliser une combinaison de mots qui riment.

N'utilise jamais de renseignements personnels ou privés dans un code d'accès ou une phrase de passe, comme des renseignements que quelqu'un peut déjà connaître ou obtenir facilement de quelqu'un d'autre.

N'utilise pas de chiffres répétitifs comme « 777 » ni de décomptes du type « 123 » ou « 321 », de dates significatives comme une date de naissance ou de numéros de téléphone. Ils sont trop faciles à deviner!

Crée des codes d'accès comportant des caractères variés! Utilise des lettres majuscules (ABC) et minuscules (abc), des chiffres (123) et des symboles (!, @, #). L'utilisation de ces quatre types de caractères crée un mot de passe super fort!

Protection des mots de passe

La création d'un mot de passe fort est très importante, mais ce n'est que la première étape pour le garder en sécurité. La deuxième étape est de le garder pour toi! Voici quelques façons de te protéger et de protéger tes mots de passe :

Utilise toujours un code d'accès unique pour chaque profil, de sorte que si un mot de passe est volé à partir d'un compte, les autres comptes resteront protégés!	Ne réutilise pas d'anciens codes d'accès – même si les anciens codes d'accès étaient associés à d'autres comptes ou profils.
La pratique exemplaire est de changer les codes d'accès de temps en temps, car même les mots de passe les plus forts peuvent finir par être devinés. Tu peux fixer une date à ton calendrier pour te le rappeler.	Ne partage pas tes mots de passe avec tes amis, même pas avec tes meilleurs amis! En fonction des règles à la maison, les mots de passe ne devraient être partagés qu'avec tes parents ou tes tuteurs, pour les situations d'urgence.
Porte attention à ton environnement physique! Fais attention que personne n'essaie de voir ton mot de passe pendant que tu le saisis dans ton ordinateur ou tes autres appareils.	Évite de te connecter à tes comptes sur les appareils d'autres personnes, car les mots de passe peuvent alors être facilement récupérés. Si c'est absolument nécessaire, assure-toi de te déconnecter des profils et des appareils une fois que tu as terminé.

C'est à ton tour!

Crée des exemples de mots de passe qui suivent les règles de « création de mots de passe forts » énumérées ci-dessus.* Essaie de créer des exemples qui sont faciles à retenir pour toi, mais difficiles à deviner pour les autres.

*Rappel! Une fois qu'un mot de passe a été écrit ou partagé avec tes pairs, il ne doit pas être utilisé comme mot de passe réel pour l'un de tes comptes en ligne!