



## Objectif

L'objectif est d'outiller les élèves afin qu'elles et ils puissent assurer leur sécurité personnelle en ligne en étant capables de reconnaître et de créer des mots de passe sécuritaires et simples à mémoriser.

## Résultats d'apprentissage

Les élèves seront en mesure :

- de reconnaître un mot de passe faible;
- de nommer les caractéristiques qui contribuent à rendre un mot de passe sécuritaire;
- de créer des mots de passe sécuritaires et simples à mémoriser pour leur propre usage en ligne;
- de rédiger une liste de pratiques à suivre pour choisir des mots de passe sécuritaires et éviter de compromettre leur sécurité en ligne.

## Glossaire

**Identifiant** : Aussi appelé *nom d'utilisateur*, l'identifiant est un code unique qui permet d'établir l'identité d'un utilisateur ou d'une utilisatrice; l'adresse courriel est souvent utilisée comme identifiant.

**Mot de passe** : « Mot » confidentiel composé d'une série de lettres, de chiffres et de caractères spéciaux qui sert de moyen d'authentification lors d'une demande d'accès.

**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.

## JEU DE CARTES

### Méli-mélo de mots de passe

(Groupes/Individuel)

#### Mise en contexte

Photocopier et découper un ensemble des cartes **Méli-mélo de mots de passe** (voir Annexe A) pour chaque élève ou groupe d'élèves. Distribuer les cartes et demander aux élèves :

- de placer les cartes en ordre croissant selon leur force/niveau de sécurité;
- de placer les cartes en ordre croissant selon leur fréquence d'utilisation parmi la population nord-américaine;
- de placer les cartes en ordre croissant selon leur facilité de mémorisation;
- d'indiquer le nombre de cartes qui représentent le genre de mots de passe qu'elles et ils utilisent ou ont déjà utilisés;
- de dire, parmi ces mots de passe, lesquels seraient acceptés sur tous les sites;
- de déterminer, parmi les mots de passe qui ne seraient peut-être pas acceptés sur tous les sites (faute d'utiliser des symboles) si ces derniers seraient encore sécuritaires si l'on éliminait le symbole qu'ils comportent.

Effectuer une mise en commun et permettre aux élèves de discuter des différences entre les résultats des différents groupes.



## DISCUSSION

(Groupe-classe/Groupes)

### Méli-mélo de mots de passe

Animer une discussion, en groupe-classe ou en petits groupes, afin de permettre aux élèves de réfléchir aux questions suivantes :

1. Quels genres mots de passe risquent de placer la sécurité d'un utilisateur ou d'une utilisatrice en danger?
  - Éléments de réponse : Ceux qui sont faciles à deviner ou qui dévoilent de l'information telle que la date de naissance/sexe.
2. Quels genres de mots de passe sont les plus faciles à deviner et pourquoi?
  - Éléments de réponse : Ceux qui sont communs ou qui comportent le nom d'un animal préféré, d'un ami ou d'une amie, d'un ou d'une enfant ou d'un conjoint ou d'une conjointe.
3. Quelles sont les caractéristiques essentielles d'un mot de passe sécuritaire?
  - Éléments de réponse : Composé de lettres, de chiffres et de symboles; comporte un minimum de huit caractères; ne comprend pas de renseignements personnels; comporte un mélange de majuscules et de minuscules (voir Annexe B).
4. Combien de mots de passe différents utilisez-vous? Quels sont les avantages et les désavantages d'utiliser le même mot de passe pour de nombreux comptes?
  - Éléments de réponse : Facilité de mémorisation, potentiel de risque/étendue des dégâts si le mot de passe est découvert.
5. Existe-t-il des contextes où il serait pertinent de divulguer ses mots de passe? Si oui, lesquels? Quelles sont les conséquences potentielles qui pourraient découler de la divulgation volontaire des mots passe?
  - Éléments de réponse : Certains parents obligent la divulgation des mots de passe afin d'autoriser l'accès aux réseaux sociaux.
6. Quelles conséquences potentielles pourraient découler de la divulgation volontaire ou de la découverte involontaire de vos mots de passe?
  - Éléments de réponse : Usurpation d'identité, vol d'argent des comptes de banque, perte d'accès aux comptes ou aux données importantes.
7. À quelle fréquence changez-vous vos mots de passe? Quelle serait la fréquence suggérée à votre avis?
  - Éléments de réponse : Certaines entreprises obligent leurs utilisateurs et utilisatrices à changer leurs mots de passe tous les trois mois, d'autres suggèrent un changement tous les six mois, l'essentiel est de changer les mots de passe souvent, surtout pour les comptes qui protègent des données importantes; de plus, on recommande de ne pas réutiliser un ancien mot de passe.
8. Quelles stratégies pourriez-vous utiliser pour vous souvenir d'un mot de passe sécuritaire, donc complexe?
  - Éléments de réponse : Utiliser uniquement les premières lettres d'une phrase ou d'une chanson préférée; ajouter des chiffres tels que le 1 pour représenter la lettre « l », le 3 pour représenter la lettre « e », le 5 pour représenter la lettre « s »; utiliser l'équivalent de deux mots connus mais écrits dans deux langues différentes avec l'ajout d'un chiffre entre les deux; utiliser un logiciel tel que lastpass.com ou 1password.com pour créer des mots de passe complexes et les mémoriser.
9. Quelles sont les mesures à prendre afin de sécuriser vos comptes si vous croyez qu'un de vos mots de passe a été découvert?
  - Éléments de réponse : Changer immédiatement son mot de passe afin de le rendre plus sécuritaire; analyser les ordinateurs à l'aide de logiciels antivirus afin de détecter les logiciels malveillants et les logiciels espion; envoyer un courriel à ses contacts afin de leur expliquer que votre compte a été piraté.



## BILLET DE SORTIE

### Mon mot de passe, ma sécurité

(Individuel)

Photocopier le **Billet de sortie : Mon mot de passe, ma sécurité** (voir **Annexe B**) et le remettre à chaque élève. Demander aux élèves de créer un mot de passe sécuritaire et de répondre aux questions.

#### Option « ère numérique »

Créer une version numérique du **Billet de sortie : Mon mot de passe, ma sécurité** et permettre aux élèves de le remplir en ligne.

## RESSOURCES COMPLÉMENTAIRES

Jeu-questionnaire iCN : Identité numérique 7-10

Écoles branchées : Qu'est-ce que l'identité numérique? (page 6), Règles de navigation responsable (page 18)

## ADAPTÉ DE LA RESSOURCE

<http://www.childnet.com/resources/know-it-all-secondary-toolkits/lower-secondary-toolkit/perfect-passwords>



## ANNEXE A – JEU DE CARTES : MÉLI-MÉLO DE MOTS DE PASSE

1

Bonjour

2

spor.ts.1989

3

Ontario

4

S01eiL

5

crocodile

6

motdepasse

7

password

8

rMp53s!jg

9

12345678

10

paulfournier



## ANNEXE B – BILLET DE SORTIE : MON MOT DE PASSE, MA SÉCURITÉ

Nom : \_\_\_\_\_

Groupe : \_\_\_\_\_

Date : \_\_\_\_\_

Crée un mot de passe sécuritaire : \_\_\_\_\_

Assure-toi que ton mot de passe :

- contient un minimum de huit caractères;
- contient des lettres et des chiffres;
- contient des lettres majuscules et des lettres minuscules;
- contient des caractères spéciaux (p. ex., %, !, \_, \*);
- ne contient pas d'information personnelle (p. ex., prénom, date de naissance, adresse).

Explique ce que tu ferais pour te souvenir d'un mot de passe comme celui-ci :

---

---

---

---

Engage-toi!

- Je m'engage à utiliser des mots de passe sécuritaires.
- Je m'engage à garder mes mots de passe confidentiels.
- Je m'engage à utiliser différents mots de passe pour mes différents comptes.
- Je m'engage à changer mes mots de passe tous les six mois.