

Habiletés en matière de configuration numérique



4^e à 6^e année

Aperçu

Les nouvelles applications, les nouveaux jeux de même que les nouveaux appareils peuvent offrir des façons emballantes aux élèves d'apprendre, de jouer et de se connecter. Mais avant de commencer, les élèves peuvent être invités à prendre des décisions concernant les renseignements qu'ils partagent, les autorisations qu'ils concèdent, les mots de passe qu'ils créent et les personnes avec qui ils interagissent.

Cette leçon présente aux élèves certains des choix auxquels ils pourraient être confrontés lors de la configuration d'une nouvelle application, d'un nouveau jeu ou d'un nouvel appareil. Les élèves en apprendront plus sur les renseignements personnels, la protection de la vie privée, les autorisations des applications, les mots de passe et les connexions en ligne, et s'exerceront à prendre des décisions sécuritaires et responsables d'entrée de jeu. En comprenant bien ce à quoi il faut porter attention pendant le processus de configuration, les élèves peuvent adopter de bonnes habitudes numériques qui les aideront à faire une utilisation plus sécuritaire et responsable de la technologie.

Résultats d'apprentissage

Les élèves seront en mesure de faire ce qui suit :

- Identifier les renseignements personnels qui devraient rester privés en ligne.
- Comprendre pourquoi les applications sollicitent des autorisations et pourquoi ils devraient réfléchir à ce qu'ils acceptent.
- Reconnaître l'importance de se doter de mots de passe robustes et privés.
- Faire des choix réfléchis quant aux personnes avec qui ils se connectent en ligne.
- Savoir quand demander de l'aide à un parent, à un tuteur, à un enseignant ou à un autre adulte de confiance.
- Acquérir des habitudes sécuritaires et responsables relativement à l'utilisation de nouvelles applications, de nouveaux jeux et de nouveaux appareils.

Préparation et matériel

- Préparer les pistes de discussion
- Préparer l'affichage ou la distribution du scénario « Configurer une nouvelle application »
- Tableau blanc ou papier-affiche
- Papier ou cahiers pour que les élèves puissent noter leurs réponses

Introduction : Commencer de manière sécuritaire

Durée : 5 à 10 minutes

Commencez en demandant aux élèves d'imaginer qu'ils viennent de télécharger une nouvelle application ou un nouveau jeu qu'ils sont impatients d'essayer.

Posez les questions suivantes :

- Que peut vous demander de faire une application avant que vous ne puissiez commencer à l'utiliser?
- Quels renseignements pourriez-vous être invités à fournir?
- Avez-vous déjà vu une application demander la permission d'utiliser une fonction de votre appareil, comme la caméra ou la fonctionnalité de localisation?
- Que pourriez-vous faire si vous n'êtes pas certain de devoir répondre « Oui »?

Expliquez que la configuration d'une application, d'un jeu ou d'un appareil implique souvent de faire des choix avant même de commencer à les utiliser. Il se peut qu'on nous demande de créer un compte, de fournir des renseignements sur nous-mêmes, de choisir un mot de passe, d'accorder l'accès à certaines parties de notre appareil ou de nous connecter avec d'autres personnes. Agir en citoyen numérique responsable signifie que l'on doit réfléchir à ces choix plutôt que de sélectionner automatiquement les options « Oui », « Autoriser » ou « Accepter ».

Discussion en classe : Que sait une application à votre sujet?

Durée : 10 à 15 minutes

Demandez aux élèves de trouver différents types de renseignements qu'une application ou qu'un jeu pourrait demander à l'étape de l'installation.

- Inscrivez leurs réponses au tableau. Exemples possibles :
- Nom
- Date de naissance
- Adresse courriel
- École
- Emplacement
- Photos
- Contacts
- Caméra / microphone

Expliquez que certains de ces éléments sont des exemples de renseignements personnels, tandis que d'autres sont des autorisations qui donnent à une application accès à des informations ou à des fonctionnalités sur un appareil. Posez les questions suivantes :

- Pourquoi une application voudrait-elle ces renseignements?
- Pourquoi une application aurait-elle besoin d'accéder à votre caméra ou à votre microphone?
- Est-ce que chaque application a besoin d'accéder à votre emplacement ou à vos contacts?
- Devriez-vous accepter automatiquement toutes les demandes d'autorisation formulées par une application?

Discutez de la mesure dans laquelle la pertinence d'une autorisation peut être fonction de l'objet de l'application. Par exemple, une application qui sert à passer des appels vidéo peut avoir besoin d'accéder à une caméra et à un microphone. Les élèves devraient réfléchir à ce que demande une application et consulter un adulte de confiance s'ils ont des doutes.

Rappelez aux élèves qu'ils n'ont pas à prendre toutes les décisions numériques seuls. Un parent, un tuteur, un enseignant ou un autre adulte de confiance peut les aider à déterminer quels renseignements ou quels accès il est approprié de fournir.

Activité : Configurer une nouvelle application

Durée : 20 à 25 minutes

Dites aux élèves d'imaginer un scénario selon lequel ils configurent une nouvelle application fictive appelée ConnectUp. Expliquez-leur qu'ils devront prendre différentes décisions au cours du processus de configuration. Pour chaque étape, les élèves doivent réfléchir à ce qu'ils feraient et pourquoi. Les élèves peuvent discuter des scénarios en petits groupes avant de partager leurs réponses avec les autres élèves de la classe.

Étape 1 :

Créer votre profil

ConnectUp vous demande ce qui suit :

- Votre prénom et votre nom de famille
- Votre date de naissance
- Votre école
- Une photo de profil
- Votre emplacement

Posez les questions suivantes aux élèves :

- Quelles informations seriez-vous à l'aise de fournir?
- Toutes ces informations sont-elles nécessaires pour utiliser l'application?
- Y a-t-il des informations que vous souhaiteriez conserver pour vous? Que pourriez-vous faire si vous n'êtes pas sûr de ce que vous devez partager?

Étape 2 :

Créer un mot de passe

Présentez trois mots de passe fictifs. Voici quelques exemples, ou créez les vôtres.

- Soccer
- Maya2015
- Rivière!Violette7Nuage

Posez les questions suivantes :

- Quel mot de passe semble le plus robuste?
- Qu'est-ce qui le rend plus difficile à deviner?
- Pourquoi l'utilisation de votre nom, de votre date de naissance ou de votre activité préférée pourrait-elle rendre un mot de passe plus facile à deviner? Pourquoi les mots de passe devraient-ils demeurer confidentiels?

Expliquez que les mots de passe robustes sont généralement plus longs, difficiles à deviner pour quelqu'un d'autre et ne reposent pas sur des renseignements personnels évidents. Les élèves devraient également éviter de partager leurs mots de passe avec leurs amis.

Étape 3 :

Choisir vos autorisations

ConnectUp demande l'autorisation d'accéder à ce qui suit :

- Appareil photo
- Microphone
- Emplacement
- Contacts

Pour chaque autorisation, posez les questions suivantes :

- Pourquoi l'application pourrait-elle vouloir y accéder?
- Est-ce logique compte tenu de ce que fait l'application?
- À quelles informations l'application pourrait-elle accéder si vous l'y autorisez? Que pourriez-vous faire si vous n'êtes pas sûr?

Rappelez aux élèves qu'ils n'ont pas à acquiescer automatiquement à chaque demande. Ils peuvent marquer une pause, réfléchir à la raison pour laquelle l'application formule cette requête et demander de l'aide à un adulte de confiance..

Étape 4 :

Établir une connexion

Vous êtes prêt à utiliser ConnectUp. Un nom d'utilisateur que vous ne reconnaissez pas vous envoie une demande de connexion. Posez les questions suivantes :

Accepteriez-vous la demande? Pourquoi ou pourquoi pas?

- Que voudriez-vous savoir avant de vous connecter avec quelqu'un? Si vous avez des amis en commun, cela signifie-t-il nécessairement que vous connaissez la personne?
- Que pourriez-vous faire si vous n'êtes pas sûr de l'identité de quelqu'un?

Discutez des raisons pour lesquelles les élèves devraient réfléchir attentivement aux personnes avec qui ils se connectent et communiquent en ligne.

Discussion en classe : notre liste de vérification pour une configuration numérique intelligente.

Durée : 10 minutes

Après avoir terminé l'activité, dites aux élèves que la classe va créer une liste de vérification qu'ils pourront utiliser la prochaine fois qu'ils essaieront une nouvelle application, un nouveau jeu ou un nouvel appareil. Écrivez le titre « Avant de commencer... » au tableau.

Demandez aux élèves de suggérer de saines habitudes basées sur ce qu'ils ont appris pendant la leçon. La liste de vérification pourrait inclure ce qui suit :

- Réfléchir aux renseignements personnels que je partage
- Garder pour moi les renseignements personnels
- Créer un mot de passe fort et le garder pour moi
- Vérifier les autorisations que demande une application
- Se demander si les autorisations sont fondées
- Faire preuve de prudence quant aux personnes avec qui je me connecte
- Demander à un adulte de confiance si je ne suis pas certain

Discutez de la façon dont ces habitudes peuvent aider les élèves à faire des choix plus sécuritaires et plus responsables dès qu'ils commencent à utiliser une nouvelle technologie.

Conclusion

Durée : 5 à 10 minutes

Posez les questions suivantes aux élèves :

- Quel est l'aspect que vous vérifieriez avant d'utiliser une nouvelle application, un nouveau jeu ou un nouvel appareil?
- Pourquoi est-il important de s'interroger quant aux renseignements que demande une application?
- Que devriez-vous faire si vous n'êtes pas certain de vouloir accorder une autorisation ou partager des renseignements?

Demandez à chaque élève d'identifier une habitude numérique future qu'il souhaite adopter au cours de l'année scolaire. Terminez en insistant sur le fait que les élèves n'ont pas besoin de connaître la réponse à chaque situation numérique. Prendre le temps de réfléchir aux renseignements qu'ils partagent, à ce qu'ils autorisent et aux personnes avec qui ils se connectent peut les aider à faire des choix plus sécuritaires et plus responsables en ligne.