digital moment numérique

Introduction à la Cybersécurité

- Niveau scolaire : 4e à 6e année du primaire et 1ère à 5e année du secondaire
- Durée : 60 minutes
- Matière : Autre
- Lien interdisciplinaire : Mathématique et Français
- Plateforme : Other
- Compétence

Dans cette leçon, nous explorerons le monde de la cybersécurité de manière simple et pratique, en utilisant des activités concrètes pour renforcer votre apprentissage et votre compréhension. Cette leçon est conçue spécifiquement pour les adolescents, leurs parents et leurs enseignants. Les élèves pourront apprendre ce qu'est la cybersécurité, pourquoi elle est importante et comment se protéger dans le monde numérique en explorant des concepts liés aux mots de passe et à l'ingénierie sociale.

digital moment numérique

Liens avec le programme de formation

Ontario

6e année : Faire des choix sains
D2. démontrer sa capacité à appliquer ses connaissances en matière de santé et ses compétences en apprentissage socio-émotionnel pour prendre des décisions raisonnées et prendre les mesures appropriées concernant sa santé et son bien-être personnels.

D2.3 appliquer des compétences d'apprentissage socio-émotionnel (p. ex., conscience de soi et compétences en autogestion, y compris la gestion de la colère ; compétences en communication, y compris l'écoute et l'affirmation de soi) pour favoriser des interactions positives et éviter ou gérer les conflits dans des situations sociales, en personne ou en ligne.

Quebec

Dimensions du Cadre de référence de la compétence numérique :
#6 : Communiquer à l'aide du numérique.
#8 : Agir en citoyen éthique à l'ère du numérique.

Objectifs

Objectifs d'apprentissage

Les élèves seront capables de...

- Expliquer ce qu'est la cybersécurité et pourquoi il est important de protéger les systèmes et les données virtuels
- Analyser des stratégies pour créer et maintenir des mots de passe robustes
- Identifier et décrire diverses méthodes d'ingénierie sociale et de piratage utilisées par des agents malveillants

Critères de réussite

Je peux...

- Définir la cybersécurité et décrire sa pertinence dans la protection des informations numériques personnelles et partagées
- Appliquer des stratégies pour créer un mot de passe unique et robuste qui maximise la sécurité
- Reconnaître les signes de l'ingénierie sociale et des tentatives d'hameçonnage (phishing)

Matériel

Matériel requis

- Présentation avec notes pour l'enseignant
- Pour certaines activités pratiques, vous aurez besoin d'une connexion Internet pour accéder aux sites suivants : Gandalf Lakera AI
- Deviner un code manuellement (Manual code guess)
- Deviner un code automatiquement (Automated code guess)
- Gouvernement du Canada Les 7 signes précurseurs de l'hameçonnage"

Matériel facultatif

- Guide des carrières en cybersécurité
- Vidéo

Cours

Activity	Description
Connaissances antérieures	Compréhension de base de l'utilisation d'un navigateur Web et de l'accès aux sites numériques. Familiarité avec le concept de mot de passe et le fait de posséder des comptes numériques personnels

	(p. ex., courriel, jeux). Sensibilisation générale aux menaces en ligne ou à la nécessité de la sécurité numérique.
Mise en train	5 minutes Envisagez de demander aux élèves de réfléchir aux questions suivantes en grand groupe : **Cybersécurité** Qu'est-ce que c'est ? Proposez votre propre définition. **Mots de passe** Qu'est-ce qui rend un mot de passe faible ou robuste ? Comment fonctionnent les mots de passe ? **Piratage (Hacking)** Quelle est la première image ou le premier mot qui vous vient à l'esprit quand vous entendez le mot pirate informatique (hacker) ?
Présentation des concepts de base	15 minutes Définissez la cybersécurité en soulignant pourquoi elle est importante et comment elle protège les utilisateurs. Utilisez les diapositives fournies, ou vos propres connaissances, pour passer en revue les trois thèmes principaux : les mots de passe, l'ingénierie sociale et le piratage. Enseignement dirigé : Naviguez vers les sites requis (p. ex., Manual Code Guess, Gandalf Lakera AI). Démontrez un exemple d'évaluation d'un mot de passe faible ou d'identification d'un signe d'hameçonnage à l'aide de la ressource fournie par le gouvernement du Canada.

Practice	**Activité 1 : Défi de robustesse des mots de passe (20 minutes) :** Dirigez les élèves vers les sites « Manual code guess » et « Automated code guess ». Mettez les élèves au défi de tester différentes structures de mots de passe (longueur, complexité, phrases) et de noter le temps ou la difficulté pour les deviner ou les pirater. Les points de discussion devraient inclure l'impact des connaissances communes sur la sécurité des mots de passe. **Activité 2 : Chasse aux signes d'hameçonnage (15 minutes) :** Les élèves consultent la ressource « Gouvernement du Canada - Les 7 signes précurseurs de l'hameçonnage ». Proposez des scénarios « Hameçonnage ou pas ? » à partir de la présentation. Demandez aux élèves d'identifier les signes précurseurs présents, en expliquant leur raisonnement basé sur leur apprentissage de l'ingénierie sociale.
Consolidation	10 minutes Animez une discussion passant en revue les critères de réussite. Demandez : « Quel est le changement que vous pouvez apporter à vos habitudes en ligne après cette leçon ? » Concluez en rappelant l'importance de la cybersécurité, en faisant référence à son lien avec des enjeux mondiaux comme les Objectifs de développement durable (ODD).
Modifications et mesures d'adaptation	1. Soutien au vocabulaire : Fournissez un glossaire des termes clés (p. ex., ingénierie sociale, hameçonnage, piratage éthique) pour une référence rapide. 2. Contenu différencié : Les plus jeunes élèves (4e à 6e année du primaire) peuvent se concentrer principalement sur la création de mots de passe et l'identification des signes de base de l'hameçonnage. Les élèves plus âgés (1ère à 5e année du secondaire) devraient analyser plus en profondeur les méthodes d'ingénierie sociale et de piratage, en utilisant les vidéos et les PDF fournis. 3. Autre forme de production : Permettez aux élèves de présenter leurs conclusions sur les signes d'hameçonnage (activité pratique 2) par des réponses écrites, une courte

	vidéo ou un organisateur graphique au lieu d'une discussion en classe.

Évaluation

Formative

Utilisez l'amorce de la mise en train comme « vérification des connaissances avant de commencer » ou outil de diagnostic pour évaluer la compréhension préalable des mots de passe, de l'ingénierie sociale et du piratage.

Prolongement

Connexions multidisciplinaires

Français : Analysez les tentatives d'hameçonnage comme des textes persuasifs, en vous concentrant sur les techniques utilisées pour tromper le destinataire (p. ex., urgence, autorité, familiarité).

Mathématiques : Explorez les mathématiques derrière la robustesse des mots de passe, en calculant la probabilité de deviner des mots de passe simples par rapport à des mots de passe complexes.

Approfondir la réflexion

1. Recherche sur le piratage éthique : Visionnez les vidéos fournies sur le piratage éthique. Recherchez et résumez la différence entre les pirates chapeau noir (black hat), chapeau blanc (white hat) et chapeau gris (grey hat). Commencez la réflexion en regardant la vidéo dans la liste de ressources.
2. Politique de cybersécurité : Rédigez une brève politique de cybersécurité personnelle ou familiale couvrant la gestion des mots de passe et la façon de répondre aux courriels ou messages suspects.