Plan d’unité de l’enseignant(e)

**Niveaux du cycle moyen**

**Ressources en matière de cybersécurité pour les enseignantes et enseignants et les éducateurs et éducatrices**

**À propos des ressources**

Ces ressources consistent en un ensemble gratuit et complet de matériel didactique, créé par des expertes et experts en cybersécurité et des éducatrices et éducateurs du Canada et directement relié au programme éducatif de l’Ontario. Disponibles pour quatre regroupements de niveaux, le langage, les objectifs d’apprentissage et les activités ont été adaptés pour les élèves du cycle primaire (1re à 3e année), du cycle moyen (4e à 6e année), du cycle intermédiaire (7e et 8e années) et du cycle secondaire (9e à 12e année).

Les ressources comprennent du matériel didactique de A à Z, tel que des plans d’unité et des rubriques recommandées pour les enseignantes et enseignants, ainsi que des feuilles de travail correspondant aux leçons pour les élèves. Les leçons abordent différents sujets essentiels liés à la citoyenneté numérique et à la cybersécurité, tels que le cyber respect et la bienveillance en ligne (la cyberintimidation), les communications sécuritaires en ligne, l’empreinte numérique positive, et plus encore!

**Utilisation des ressources**

Le but de ces ressources est de fournir au corps enseignant de l’Ontario un ensemble moderne de matériel lié au programme d’études, donnant les moyens et préparant à doter les jeunes des connaissances et des outils dont ils ont besoin pour utiliser la technologie de façon positive, et pour être aussi en mesure d’identifier et de prévenir les risques connexes.

Ces ressources sont accessibles et peuvent facilement être mises en œuvre, tant dans une salle de classe physique que dans un environnement virtuel.

De façon proactive, le catalyseur a offert deux versions de chaque ressource :

1. **Une version PDF** se voulant une ressource téléchargeable et prête à l’utilisation pour les éducatrices, les éducateurs, les enseignantes et les enseignants. Téléchargez, imprimez et partagez des copies papier ou numériques avec les élèves pour une utilisation instantanée.
2. **Une version Microsoft Word**, dont le contenu est le même que la version PDF. Toutefois, la version Word est modifiable, ce qui permet au corps enseignant de changer le langage ou les feuilles de travail selon le besoin. Il est recommandé de modifier les plans d’unité et les leçons de façon à les adapter aux habiletés et aux besoins d’apprentissage de vos élèves, ou pour incorporer aux leçons des modalités supplémentaires ou privilégiées.

**Ressources supplémentaires en cybersécurité**

La cybersécurité et la citoyenneté numérique sont des domaines d’étude relativement nouveaux et, bien que ces ressources aient été mises au point en présumant une expérience technique ou cybernétique potentiellement limitée, nous reconnaissons qu’il peut être nécessaire d’obtenir des renseignements supplémentaires pour mieux comprendre les sujets abordés.

Nous encourageons le corps enseignant à mener des recherches indépendantes et à profiter de la multitude de ressources gratuites disponibles en ligne, y compris les ressources pour les jeunes de Rogers Cybersecure Catalyst : <https://cybersecurite.lecentrefranco.ca/>

**À propos de l’organisme**

Rogers Cybersecure Catalyst, le « catalyseur », est un organisme sans but lucratif détenu et exploité par Ryerson University. Le catalyseur s’efforce de donner aux citoyens et aux entreprises du Canada les moyens de tirer pleinement parti des possibilités offertes dans l’espace virtuel et de relever les importants défis liés à la cybersécurité, par la formation et la certification, l’accélération commerciale et le soutien aux cyberentreprises, la recherche et le développement appliqués et l’éducation publique.

**À propos de l’initiative**

En 2019, Rogers Cybersecure Catalyst a conclu un partenariat avec Rogers Communications inc. pour aider à développer un écosystème canadien de cybersécurité et à contribuer à la prospérité de l’économie numérique du Canada. En tant qu’entreprise de pointe dans le domaine de la technologie et des médias, Rogers s’engage à protéger la cybersécurité des Canadiens et Canadiennes.

Ensemble, le catalyseur et Rogers ont déterminé le besoin de favoriser une collaboration plus étroite entre la communauté de la cybersécurité, le milieu universitaire et les partenaires en éducation, afin de sensibiliser et de mieux comprendre la cybersécurité, en particulier chez les jeunes.

**Attentes générales en ce qui concerne le curriculum de l’Ontario, Français**

|  |  |  |  |
| --- | --- | --- | --- |
| **Communication** **orale** | **Écriture** | **Médias** **et littératie** | **Santé et éducation physique** |
| **1.** **Écouter pour comprendre :** Écouter afin de comprendre et de réagir de façon appropriée dans diverses situations et à diverses fins;  **2.** **Parler pour communiquer :** Utiliser des stratégies et des compétences en expression orale de façon appropriée pour communiquer avec différents publics et pour atteindre une variété d’objectifs;  **3.** **Réfléchir aux stratégies et aux compétences :** Prendre en considération et déterminer leurs points forts, du point de vue de l’auditeur et de celui du locuteur, les points à améliorer et les stratégies qui ont été jugées les plus utiles dans les situations de communication orale. | **1.** **Développement et organisation du contenu :** Générer, rassembler et organiser des idées et de l’information pour rédiger à l’intention d’un auditoire et d’un objectif précis;  **2.** **Utilisation des connaissances de la forme et du style :** Rédiger et réviser ses écrits, au moyen d’une gamme d’éléments littéraires, informatifs, graphiques et stylistiques appropriés à l’objectif et au public;  **3.** **Application de la connaissance des conventions :** Utiliser des compétences et des stratégies d’édition, de révision et de publication, et la connaissance des conventions linguistiques, pour corriger les erreurs, peaufiner le texte et présenter efficacement le travail;  **4.** **Réfléchir aux stratégies et aux compétences :** Prendre en considération et déterminer leurs points forts en tant que rédacteurs, les points à améliorer et les stratégies qu’ils ont jugées les plus utiles à différentes étapes du processus de rédaction. | **1.** **Compréhension des textes médiatiques :** Démontrer une compréhension de divers textes médiatiques;  **2.** **Comprendre les formats, conventions et techniques des médias :** Nommer certains formats médiatiques et expliquer comment les conventions et les techniques qui leur sont associées sont utilisées pour conférer une signification;  **3.** **Créer des textes médiatiques :** Créer divers textes médiatiques destinés à des fins et à des publics différents, en utilisant les formats, conventions et techniques appropriés;  **4.** **Réfléchir aux stratégies et aux compétences :** Prendre en considération et déterminer leurs points forts, du point de vue du créateur et de celui de l’interprète médiatique, les points à améliorer et les stratégies qui ont été jugées les plus utiles pour comprendre et créer des textes médiatiques. | **1.** **Aptitudes à l’apprentissage social et émotionnel :** Appliquer, au mieux de ses capacités, une gamme de compétences d’apprentissage socioémotionnelles au fil de l’acquisition des connaissances et des compétences liées aux attentes des volets Vie active, Compétence des mouvements et Vie saine pour ce niveau;  **2.** **Vie saine :** Démontrer la capacité d’établir des liens qui se rapportent à la santé et au bien-être, comment leurs choix et leurs comportements ont une incidence sur eux-mêmes et sur les autres, et la façon dont les facteurs dans le monde qui les entoure affectent leur santé et leur bien-être et ceux des autres. |

**Tâche sommative : Infographie de la citoyenneté numérique**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Catégorie** | Niveau 4 | Niveau 3 | Niveau 2 | Niveau 1 |
| **Connaissance** | Démontre une connaissance approfondie du thème choisi en cybersécurité  Utilise 5 sources d’information ou plus | Démontre une bonne connaissance du thème choisi en cybersécurité  Utilise 3 ou 4 sources d’information | Démontre une certaine connaissance du thème choisi en cybersécurité  Utilise des sources d’information limitées | Démontre une connaissance limitée du thème choisi en cybersécurité  Preuves de recherche limitées |
| **Réflexion** | Utilise des compétences de conception graphique, telles que des graphismes éclatants, avec une grande efficacité | Utilise des compétences de conception graphique, telles que des graphismes éclatants, avec efficacité | Utilise des compétences de conception graphique, telles que des graphismes éclatants, avec une certaine efficacité | Utilise des compétences de conception graphique, telles que des graphismes éclatants, avec une efficacité limitée |
| **Communication pour différents publics et objectifs** | Communique le message voulu au public avec une grande efficacité  Idée principale claire et renseignements complémentaires stimulants | Communique le message voulu au public avec efficacité  Idée principale claire et renseignements complémentaires adéquats | Communique le message voulu au public avec une certaine efficacité  Idée principale avec renseignements complémentaires qui manquent de clarté | Communique le message voulu au public avec une efficacité limitée  Idée principale floue |
| **Application des connaissances et des compétences** | Applique ses connaissances et ses compétences en recherche à de nouveaux contextes (infographie) avec une grande efficacité | Applique ses connaissances et ses compétences en recherche à de nouveaux contextes (infographie) avec efficacité | Applique ses connaissances et ses compétences en recherche à de nouveaux contextes (infographie) avec une certaine efficacité | Applique ses connaissances et ses compétences en recherche à de nouveaux contextes (infographie) avec une efficacité limitée |

**Rétroaction de l’enseignante ou de l’enseignant** :

**Note finale** :

**Aperçu de l’unité**

Cette unité est conçue pour enseigner aux jeunes élèves comment être les gardiennes et gardiens de la citoyenneté numérique dans leurs communautés de classe et dans la communauté numérique au-delà de la salle de classe. La citoyenneté numérique désigne l’utilisation responsable et sécuritaire des technologies et de l’Internet par quiconque les utilise pour interagir avec la société.

Des évaluations seront faites tout au long de cette unité, qui mène à une tâche sommative : une infographie développée par les élèves (une publicité ou une représentation visuelle de l’information) sur l’un des six sujets enseignés dans cette unité, ou au-delà, selon que vous souhaitez faire de cette tâche une tâche axée sur la recherche.

**Aperçu des leçons**

Leçon 1 : Cyberrespect et bienveillance en ligne

Leçon 2 : Empreinte numérique positive

Leçon 3 : Communication sécuritaire en ligne

Leçon 4 : Mots de passe et codes d’accès

Leçon 5 : La vérité en ligne

Leçon 6 : Infographie sur la citoyenneté numérique

Ressources pour les enseignantes et enseignants : Rubrique infographique

Pour de plus amples renseignements sur les sujets abordés ou pour du matériel d’appoint supplémentaire, consultez les ressources téléchargeables pour les jeunes de Rogers Cybersecure Catalyst :

<https://cybersecurite.lecentrefranco.ca/>

**Leçon 1 : Cyber respect et bienveillance en ligne**

**Plan de leçon pour les parents ou tutrices et tuteurs**

La culture numérique est un élément fondamental du 21e siècle; elle est essentielle à la participation civique et sociale, à l’accès aux services publics et à la réussite dans une économie numérique (comme l’explique une [récente publication](https://brookfieldinstitute.ca/the-importance-of-accessible-and-inclusive-public-service-tech-in-times-of-crisis/) du Brookfield Institute - en anglais seulement). Par conséquent, dans cette unité, les élèves se familiariseront avec la citoyenneté numérique et apprendront comment gérer leur présence numérique en évolution.

Aujourd’hui, les élèves examineront de près comment communiquer et exister en ligne avec respect. Elles et ils apprendront comment reconnaître les interactions négatives en ligne (cyberintimidation) et y réagir, et comment présenter son meilleur « profil numérique ».

|  |  |
| --- | --- |
| **Accroche**  10 minutes | *Accueillir les élèves à leur entrée dans la classe*  *Excellente occasion de faire le point sur le bien-être*  Cyberrespect et bienveillance en ligne  (Tableau « savoir, vouloir et apprendre »)  Évaluer ce que les élèves savent déjà sur la cyberintimidation, le cyberrespect et la bienveillance en ligne et déterminer ce qui pique naturellement leur curiosité, en remplissant le tableau « savoir, vouloir et apprendre » dans le document de la leçon 1 correspondant.  **Suggestion** : Partager une définition de la cyberintimidation et de la bienveillance en ligne pour orienter les discussions en classe lors de l’examen de ce que les élèves ont écrit ou dessiné dans leur document.  **Exemples de définitions :**  **Cyberintimidation**: Lorsqu’une personne (ou un groupe) fait preuve de méchanceté envers une autre personne sur Internet ou par le biais d’une technologie (comme un téléphone cellulaire ou une tablette). Il peut s’agir d’insulter, de répandre des rumeurs, de forcer une personne à faire quelque chose qu’elle ne veut pas faire ou de se moquer de quelqu’un et de faire en sorte que d’autres le fassent également.  **Exemples suggérés** :   * Publier des choses méchantes (mots, émoticônes ou photos) en ligne qui s’adressent à une personne ou qui sont à propos d’une personne, dans le but de blesser ses sentiments. * Utiliser le profil en ligne d’une autre personne pour publier des choses embarrassantes à son sujet. * Publier des photos ou vidéos embarrassantes d’une personne. * Messages blessants pour une personne publiés en ligne ou envoyés à quelqu’un d’autre.   **Bienveillance en ligne** : Utiliser Internet de façon positive, comme pour écrire des messages gentils sur les médias sociaux ou pour partager des photos et des vidéos en ligne pour égayer la journée d’une autre personne.  **Exemples suggérés** :   * Traitons toujours les autres comme nous voulons être traités. * Traitez les autres avec gentillesse en tout temps - il est toujours plus facile d’être gentil que d’être méchant. * Lorsque vous voyez une personne être gentille avec quelqu’un d’autre, faites-lui un compliment et aidez-la à se sentir bien à l’idée d’être gentil.   Que sais-tu déjà et que veux-tu apprendre? Nous allons remplir le tableau de ce que nous avons appris au fur et à mesure.  **Cyberrespect et bienveillance en ligne**  Qu’est-ce que je sais?  Qu’est-ce que je veux savoir? |

|  |  |
| --- | --- |
| **Objectifs d’apprentissage et critères de réussite**  5 minutes | Communiquer les objectifs d’apprentissage pour un apprentissage ciblé. Les critères de réussite renseignent les élèves sur ce qu’elles et ils seront en mesure de faire une fois la matière apprise.  **Objectifs d’apprentissage** :   * Je sais reconnaître le cyberrespect et la bienveillance en ligne. * Je sais comment répondre aux interactions négatives en ligne. * Je sais reconnaître l’intimidation en ligne (cyberintimidation). * Je ne reste pas indifférente ou indifférent. |
| **Données et modélisation** | *Enseigner et montrer le contenu et les compétences que les élèves doivent connaître pour réussir.* *Faire une modélisation à l’aide d’exemples qui éclairent la compréhension.*   * Le cyberrespect ressemble à..., donne un sentiment de..., ne donne pas un sentiment de... * La bienveillance en ligne ressemble à..., donne un sentiment de..., ne donne pas un sentiment de...   Les élèves peuvent faire un remue-méninges pour trouver des exemples de bienveillance en ligne en remplissant le tableau de façon individuelle, en groupe, puis en classe.  En permettant aux élèves de partager des expériences qui les concernent, vous aurez une idée de leur présence en ligne. Par exemple, si de nombreux étudiants donnent des exemples de jeux en ligne, vous pouvez modeler en fonction des jeux l’information que vous partagez. |

|  |  |
| --- | --- |
| **Pratique guidée et autonome**  20 minutes | ***Observer, inviter, soutenir, enrichir***  Examiner la définition d’un « acteur » et comment celui-ci est différent d’un « spectateur ».  **Exemples de définitions** :   * **Acteur** : Une personne qui prend la parole ou qui agit en faveur d’une personne qui a besoin d’aide. * **Spectateur** : Une personne qui est témoin ou au courant d’une situation blessante qui se produit, mais qui décide de ne pas intervenir.   En petits groupes, demander aux élèves de discuter des raisons pour lesquelles une personne peut se sentir mal à l’aise d’être un « acteur ». Les réponses possibles peuvent être les suivantes :   * *Le « spectateur » a peut-être déjà été victime d’intimidation et ne veut pas risquer de se faire de nouveau intimider.* * *Le « spectateur » ne sait peut-être pas quoi dire.* * *Le « spectateur » ne pense peut-être pas qu’il est de sa responsabilité d’intervenir.*   Ce n’est pas toujours facile ou simple de choisir de se mobiliser pour ce qui est juste, mais il est toujours important de le faire.  **Discussion** : Bien que l’on puisse se sentir mal à l’aise d’être un « acteur », c’est une excellente option pour lutter contre la cyberintimidation.  **Renforcement facultatif** : Fournir des exemples de façons d’être un « acteur » et en discuter. Voici quelques exemples suggérés :   * Si les élèves connaissent la personne qui fait de l’intimidation, elles et ils peuvent aider cette personne à voir la bienveillance en faisant preuve de bienveillance envers elle, par exemple en publiant quelque chose de positif à son sujet ou en l’invitant à rejoindre une communauté en ligne. * Les élèves peuvent se regrouper avec des amies et amis, des camarades de classe ou des coéquipières et coéquipiers qui veulent aussi être des « acteurs » - un groupe de personnes positives qui se soutiennent les unes les autres peut faire une grande différence pour quelqu’un qui a été blessé par un intimidateur!   **Remarques importantes** :   * **Rappeler aux élèves qu’ils ne devraient pas affronter un intimidateur qui est un étranger, ni en personne ni en ligne.** **Au lieu de cela, ils devraient le signaler à un parent ou à une tutrice ou un tuteur, à une enseignante ou un enseignant ou à une ou un autre adulte de confiance.** * **Rappeler aux élèves qu’elles et ils peuvent toujours communiquer avec Jeunesse, J’écoute en envoyant un message texte au 686868 ou en composant le 1-800-668-6868 de partout au Canada, 24 heures sur 24, 7 jours sur 7.** |
| **Vérification de la compréhension**  10 minutes | ***Observations, évaluation formative***  Réponse à la documentation pour la leçon 1 :  Qu’est-ce qui pourrait faire en sorte qu’une ou un élève se sente mal à l’aise d’être un « acteur »? |
| **Conclusion** | *Révision, questions, conclusion, discussion, appréciations*  Un tableau des sentiments liés à la bienveillance en ligne peut servir de guide ou de contrat pour la communauté de classe alors qu’elle évolue dans l’espace numérique.  Vous pourriez créer un tableau aide-mémoire ou un contrat pour que tous les élèves le signent, qui comprendrait les sentiments que votre classe a relevés. |

|  |  |
| --- | --- |
| **Ressources** |  |
| **Évaluation** | *Pour l’apprentissage* :   * Observation ✔ * Notes anecdotiques * Liste de vérification * Entretiens et conversations * Exemples de travaux/produits ✔ * Suivis ✔   *En tant qu’apprentissage :*   * Rubrique * Critères de réussite ✔ * Introspection * Autre : La réponse de l’élève peut servir de billet de sortie ✔   *De l’apprentissage :*   * Jeu-questionnaire * Examen * Présentation * Affectation * Autre produit |
| **Remarques** : |  |

**Leçon 2 : Empreinte numérique positive**

**Plan de leçon pour les parents ou tutrices et tuteurs**

Les élèves ont de nombreuses raisons d’avoir une empreinte numérique positive; c’est-à-dire l’impression que les élèves laissent derrière elles et eux après avoir fait une publication en ligne, publié des messages dans un espace de clavardage collectif ou participé à d’autres activités en ligne. Une fois qu’une chose est publiée en ligne, elle y reste, il est donc important que les élèves soient très conscientes et conscients de leurs actions en ligne.

Les élèves apprendront comment leurs actions en ligne affectent leurs proches et comment construire des empreintes numériques responsables et positives qui les représenteront de manière appropriée.

|  |  |
| --- | --- |
| **Accroche**  10 minutes | *Accueillir les élèves*  *Excellente occasion de faire le point sur le bien-être*  *Mettre à contribution les connaissances antérieures*  La façon dont vous vous conduisez en ligne est votre empreinte numérique. Il s’agit de tout ce que vous publiez ou aimez en ligne, et de ce qui se passe lorsque votre nom fait l’objet d’une recherche.  Les élèves ont de nombreuses raisons d’avoir une empreinte numérique positive, car ils se représentent eux-mêmes et représentent leur famille, leur école et leur communauté.  **Voici quelques suggestions aux fins de discussion**:  Qu’est-ce qui pourrait mener à une empreinte numérique négative?  Voici quelques exemples :   * Dire des choses méchantes sur d’autres personnes dans un message texte, dans un espace de clavardage, etc. (c’est-à-dire, la cyberintimidation) * Envoyer ou partager des photos, des vidéos, des images ou des publications inappropriées * Choisir des noms d’utilisateur ou des adresses de courriel grossiers ou déplaisants   **Comment créer une empreinte numérique positive?** Voici quelques exemples :   * Être gentil et respectueux envers les autres en tout temps. * Garder ses publications positives (p. ex., souligner des compétences particulières, aider les autres, etc.). * L’humour est un outil pratique et formidable, mais les enfants doivent faire preuve de prudence! Leur conseiller de garder l’humour léger et positif en évitant les sujets délicats et de ne jamais utiliser l’humour pour rire aux dépens de quelqu’un d’autre.   Présenter la documentation de la leçon 2 *Répercussions de vos actions en ligne* et donner des exemples de la façon dont les actions d’une personne en ligne ont des répercussions.  Par exemple, le partage d’une réalisation peut rendre vos parents fiers, mais le partage de renseignements sur le lieu où vous vous trouvez pourrait les inquiéter beaucoup.  **Renforcement facultatif** :  Pensez à lire le livre graphique *Ping* d’Ani Castillo, et discutez du fait que vous ne pouvez contrôler que ce que vous exposez dans le monde.  Vous pouvez choisir d’acquérir le livre à l’avance, ou de regarder une vidéo d’Ani Castillo lisant son livre ici : https://www.youtube.com/watch?v=fqTZe3T0\_uQ (en anglais, sous-titré en espagnol).  Les messages et les thèmes sont un excellent point de départ pour discuter d’une empreinte numérique positive, et d’une bonne citoyenneté numérique et dans la vie réelle. |
| **Objectifs d’apprentissage et critères de réussite**  5 minutes | Communiquer les objectifs d’apprentissage pour un apprentissage ciblé. Les critères de réussite renseignent les élèves sur ce qu’elles et ils seront en mesure de faire une fois la matière apprise.  **Objectifs d’apprentissage** :   * Je comprends que j’ai une responsabilité envers mes amis, ma famille, ma communauté et moi-même de créer une empreinte numérique positive. * Je connais des stratégies pour construire une empreinte numérique positive et réparer une empreinte endommagée. |
| **Données et modélisation** | *Inscrire ici les remarques à l’attention de la Gestion des locaux (matériel supplémentaire).*   * *Contenu* * *Processus* * *Environnement d’apprentissage* * *Produit*   Une fois que les élèves ont travaillé sur le document intitulé Leçon 2 - *Répercussions de vos actions en ligne*, leur demander d’ajouter d’autres exemples en travaillant avec une ou un partenaire et de faire part de quelques exemples à la classe. |
| **Pratique guidée et autonome**  20 minutes et plus | *Observer les élèves qui travaillent ensemble pendant le travail de groupe.*  S’il y a du temps, demander aux élèves de relire la section « Comment créer une empreinte numérique positive » et de répondre à la question supplémentaire à la fin du document.  Cela peut être utilisé comme évaluation de l’apprentissage. |
| **Vérification de la compréhension**  10 minutes | Répondre à la question suivante : *Pouvez-vous imaginer d’autres façons de construire votre empreinte numérique positive?* |
| **Conclusion** | Partager les réponses des élèves.  Exprimer votre gratitude aux élèves pour avoir partagé ouvertement leurs pensées à propos d’un sujet important. |
| **Ressources** | Ressources pour l’éducatrice ou l’éducateur |
| **Évaluation** | Pour l’apprentissage :   * Observation ✔ * Notes anecdotiques ✔ * Liste de vérification * Entretiens et conversations ✔ * Exemples de travaux/produits ✔ * Suivis   En tant qu’apprentissage :   * Rubrique * Critères de réussite * Introspection * Autre   De l’apprentissage :   * Jeu-questionnaire * Examen * Présentation * Affectation * Autre produit |
| Remarques : |  |

**Leçon 3 : Communication sécuritaire en ligne**

**Plan de leçon pour les parents ou tutrices et tuteurs**

L’utilisation de la technologie présente de nombreux avantages dont les élèves et leurs familles sont déjà bien conscients. Aujourd’hui, nous informons les élèves de certaines mesures de sécurité en ligne, afin qu’elles et ils puissent continuer à profiter de l’espace en ligne avec moins de facteurs de risque.

|  |  |
| --- | --- |
| **Accroche**  10 minutes | *Accueillir les élèves*  *Excellente occasion de faire le point sur le bien-être*  *Mettre à profit les connaissances antérieures, rappel de la leçon précédente*  Dans la leçon précédente, nous avons discuté de nos empreintes numériques et de la façon de créer une présence en ligne qui nous représente de façon positive. Aujourd’hui, nous apprendrons comment être en sécurité en ligne et nous deviendrons conscients des risques encourus lorsque nous clavardons ou échangeons des renseignements avec d’autres personnes, tout en nous amusant!  **Activité « Pouce vers le haut / Pouce vers le bas »**  Demander aux élèves de répondre « oui » avec un pouce vers le haut et de répondre « non » avec un pouce vers le bas pour évaluer leur expérience de présence en ligne.   * Je possède un compte sur une console ou un site de jeux (PlayStation, Xbox, etc.). * J’ai ma propre adresse de courriel ou un compte en ligne. * J’ai mon propre profil de médias sociaux (Snapchat, TikTok, etc.). * Je possède ou j’utilise un appareil électronique tel qu’un ordinateur portable, une tablette ou un téléphone portable.   Selon les résultats obtenus dans votre classe, diriger une discussion sur certains des risques associés à ces activités et au partage de renseignements personnels en ligne.  Demander aux élèves de faire part de leurs habitudes, à savoir quand et comment ils utilisent leurs appareils, que ce soit à la maison ou à l’école. |
| **Objectifs d’apprentissage et critères de réussite**  5 minutes | Communiquer les objectifs d’apprentissage pour un apprentissage ciblé. Les critères de réussite renseignent les élèves sur ce qu’elles et ils seront en mesure de faire une fois la matière apprise.  **Objectifs d’apprentissage** :   * Je connais des stratégies pour me protéger des risques en ligne. * Je peux reconnaître les communications dangereuses en ligne. |
| **Données et modélisation** | À cet âge, le temps passé en ligne comprend souvent le bavardage avec des amis, le partage de photos, le jeu ou le visionnement de vidéos. Certaines de ces activités ont lieu à l’aide de plateformes de médias sociaux, d’applications mobiles ou d’un système de messagerie qui permet aux enfants d’avoir des conversations avec des gens qu’elles ou ils n’ont peut-être jamais rencontrés en personne ou qu’elles et ils ne connaissent pas très bien. Dans de tels cas, il est difficile de savoir qui sont les personnes qui se trouvent à l’autre bout de l’appareil, ou quelles sont leurs intentions. C’est pourquoi, pour communiquer en ligne en toute sécurité, il est important de limiter la quantité de renseignements privés partagée publiquement, car des inconnus peuvent essayer d’utiliser cette information pour créer de fausses amitiés dans l’espoir de gagner quelque chose de personnel sur l’enfant et d’utiliser cette information pour lui causer du tort.  En ligne, les élèves devraient toujours faire preuve de vigilance et être à l’affût des « charmeurs en ligne ».  **Exemple de définition** :  **Charmeur** : Une personne qui a une personnalité agréable, qui semble amicale et décontractée, mais qui utilise habituellement son charme pour manipuler les autres. Les charmeurs en ligne ne sont pas faciles à repérer parce qu’ils donnent souvent l’impression d’être réellement gentils. Ils utilisent les renseignements privés d’une personne, ou comment elle se sent, comme une occasion de gagner sa confiance.  Afin d’aider les enfants à déterminer si elles ou ils sont en train de communiquer avec un charmeur en ligne potentiel en utilisant des appareils, leur expliquer qu’elles ou ils devraient rester à l’affût des charmeurs et informer un parent, une tutrice ou un tuteur, une enseignante ou un enseignant ou une ou un autre adulte de confiance si les situations suivantes se produisent :   * Quelqu’un commence par leur poser des questions simples, mais devient ensuite plus personnel. * Quelqu’un les complimente, prétend aimer toutes les mêmes choses ou leur offre de leur acheter des choses; c’est souvent une astuce pour gagner la confiance des enfants! * Quelqu’un essaie d’amener les enfants à se sentir assez en sécurité pour se rencontrer en personne, participer à une discussion vidéo ou s’envoyer des photos.   **Conseils à offrir aux enfants lorsqu’ils communiquent avec d’autres en ligne :**   * Encourager les enfants à faire confiance à leur instinct! Si une chose ou une personne leur semble « effrayante » ou les met mal à l’aise, même si les enfants ne comprennent pas pourquoi, elles et ils devraient écouter ce sentiment. Expliquer aux enfants que ce sentiment se produit souvent quand, au fond, elles et ils savent que quelque chose ne va pas.   **Si l’enfant pense qu’elle ou il est potentiellement en communication avec un charmeur, elle ou il devrait prendre les mesures suivantes\* :**   * **ARRÊTER**: Arrêter de parler au charmeur immédiatement. * **BLOQUER** : Bloquer la conversation avec le charmeur, mais ne pas supprimer les messages; partager plutôt ces messages avec un adulte de confiance. * **PARLER** : Parler immédiatement à un parent ou une tutrice ou un tuteur, à une enseignante ou un enseignant ou à une ou un autre adulte de confiance.   *\*Voir l’infographie dans le document de la leçon 3*  **Voici des exemples d’amorces de conversation en classe**:   * Quels sont les moyens de reconnaître un charmeur en ligne? * Qu’est-ce que l’on considère comme des renseignements personnels ou privés? * Quelles mesures pouvez-vous prendre pour rester en sécurité en ligne? |
| **Pratique guidée et autonome**  20 minutes | *Observer, inviter, soutenir, enrichir*  Donner aux élèves le temps de créer leur affiche d’information sur la communication en ligne sécuritaire. |
| **Vérification de la compréhension**  10 minutes | *Observations, évaluation formative*  S’assurer d’être disponible pour répondre aux questions des élèves. Selon le thème de leur affiche, les élèves pourraient avoir besoin d’un certain soutien pour rendre leur information positive et valorisante. |
| **Conclusion** | *Révision, conclusion, discussion et appréciations*  *Avez-vous déjà eu un sentiment étrange à propos de quelqu’un ou de quelque chose en utilisant la technologie?* *Qu’est-ce qui rendait la chose ou la personne étrange?* *À quelle personne l’as-tu dit?*  **Conseil** : Essayer d’utiliser des comparaisons de situations en personne pour expliquer un sentiment d’instinct - par exemple lorsque quelqu’un nous fixe trop longtemps du regard ou nous suit physiquement de trop proche.  **Discuter** : *Qu’est-ce que l’on considère comme des renseignements personnels ou privés?* *Pourquoi est-il dangereux de partager ce type d’information en ligne ou avec des personnes inconnues?* |
| **Ressources** | Ressources pour l’éducateur ou l’éducatrice |
| **Évaluation** | Pour l’apprentissage :   * Observation✔ * Notes anecdotiques * Liste de vérification * Entretiens et conversations✔ * Exemples de travaux/produits * Suivis   En tant qu’apprentissage :   * Rubrique * Critères de réussite * Introspection * Autre   De l’apprentissage :   * Jeu-questionnaire * Examen * Présentation * Affectation * Autre produit |
| Remarques : |  |

**Leçon 4 : Mots de passe et codes d’accès**

**Plan de leçon pour les parents ou tuteurs**

Qu’est-ce qu’un code d’accès? Les codes d’accès (aussi appelés mots de passe) sont comme des clés pour protéger ses renseignements personnels et privés des autres. Les codes d’accès peuvent être une série de mots aléatoires; une phrase mémorable ou une combinaison de mots, de nombres ou de symboles unique à l’utilisateur. Tout comme une empreinte digitale!

Aujourd’hui, nous informons les élèves à propos des mots de passe forts et des moyens pour protéger leurs renseignements en ligne.

|  |  |
| --- | --- |
| **Accroche**  10 minutes | *Accueillir les élèves*  *Excellente occasion de faire le point sur le bien-être*  *Mettre à contribution les connaissances antérieures*  Faire un remue-méninges pour déterminer *où* les mots de passe sont utilisés.  Faire un remue-méninges pour déterminer *pourquoi* nous utilisons des mots de passe.  Tenir une séance de remue-méninges sur les mots de passe les plus populaires.  *Peut-être fait avec toute la classe, en petits groupes ou avec une ou un partenaire.*  **Exemple de définition** :  **Codes d’accès** : Imaginer les codes d’accès (plus communément « mots de passe »)  comme les clés d’une maison. Personne ne peut utiliser ses clés pour entrer dans la maison de quelqu’un d’autre parce que les clés sont uniques selon leur forme, leur longueur et leur nombre de rainures; la clé de la demeure protège le détenteur de la clé, sa famille et ses biens. Les codes d’accès sont des clés qui permettent de protéger les renseignements personnels et privés en ligne des autres. Les codes d’accès peuvent être une série de mots aléatoires; une phrase mémorable ou une combinaison de mots, de nombres ou de symboles uniques à l’utilisateur. Tout comme une empreinte digitale!  Selon [Splash Data](https://rockit.cloud/2020/03/18/the-most-commonly-used-password-in-2020-is/), certains des mots de passe les plus populaires en 2020 étaient :   * 123456 * 123456789 * password * 1234567 * 12345678 * 12345 * iloveyou * 111111 * 123123 * Password1 |
| **Objectifs d’apprentissage et critères de réussite**  5 minutes | Communiquer les objectifs d’apprentissage pour un apprentissage ciblé. Les critères de réussite renseignent les élèves sur ce qu’elles et ils seront en mesure de faire une fois la matière apprise.  **Objectifs d’apprentissage :**   * Je peux créer un mot de passe fort et sécurisé. * Mes mots de passe ne sont pas faciles à deviner. * Je sais comment protéger mon mot de passe des autres. |
| **Données et modélisation** | Enseigner et montrer le contenu et les compétences que les élèves doivent connaître pour réussir. Faire une modélisation à l’aide d’exemples qui éclairent la compréhension.  *Inscrire ici les remarques à l’attention de la Gestion des locaux (matériel supplémentaire).*   * *Contenu* * *Processus* * *Environnement d’apprentissage* * *Produit*   Apprendre aux élèves à protéger leurs empreintes numériques et leurs renseignements personnels en protégeant leurs mots de passe. À l’aide du document comme guide, examiner comment créer un mot de passe fort.  **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 se remémorer. Si tu as besoin d’aide pour en trouver un, 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 secrète, comme de l’information que quelqu’un peut déjà connaître ou obtenir facilement d’une autre personne. * N’utilise pas de chiffres répétitifs comme « 777 », ni un décompte du type « 123 » ou « 321 », ni un nombre significatif comme une date de fête ou un numéro de téléphone. Ceux-là sont trop faciles à deviner! * Crée des codes d’accès comportant des caractères variés! Inclus 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!   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 pour les enfants de se protéger eux-mêmes et de protéger leurs mots de passe :  **Protection des 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 ces 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! Selon les règles à la maison, les mots de passe ne devraient être partagés qu’avec tes parents et avec tes tutrices et tuteurs, pour les situations d’urgence. * Porte attention à ce qui t’entoure! 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. |
| **Pratique guidée et autonome**  20 minutes | *Observer, inviter, soutenir, enrichir*  Demander aux élèves de créer leurs propres exemples de mots de passe qui suivent les pratiques exemplaires décrites dans le document de la leçon 4 - des mots de passe qui seraient faciles à retenir pour l’élève, mais difficiles à deviner pour les autres.  **Remarque importante : Rappeler aux élèves que, selon leurs règles à la maison, ils pourraient devoir partager leurs mots de passe avec leurs parents ou leurs tutrices ou tuteurs.** |
| **Vérification de la compréhension**  10 minutes | *Observations, évaluation formative*  **Renforcement facultatif** :  Vérifier la force des exemples de mots de passe des élèves grâce à l’outil en ligne [*Kaspersky Password Checker*](https://password.kaspersky.com/fr/)*:* [*https://password.kaspersky.com/fr/*](https://password.kaspersky.com/fr/). |
| **Conclusion** | *Révision, conclusion, discussion et appréciations*  Partager des exemples de mots de passe, discuter de la force des mots de passe et de la façon dont les exemples pourraient être améliorés, pour inspirer la classe. Rappeler aux élèves qu’une fois qu’un mot de passe a été écrit ou partagé avec des pairs, il ne devrait pas être utilisé comme mot de passe réel pour l’un de leurs comptes en ligne! |
| **Ressources** | Ressources pour l’éducateur ou l’éducatrice |
| **Évaluation** | Pour l’apprentissage :   * Observation ✔ * Notes anecdotiques * Liste de vérification * Entretiens et conversations * Exemples de travaux/produits * Suivis   En tant qu’apprentissage :   * Rubrique * Critères de réussite * Introspection * Autre : Mot de passe vérifié ✔   De l’apprentissage :   * Jeu-questionnaire * Examen * Présentation * Affectation * Autre produit |
| Remarques : |  |

**Leçon 5 : La vérité en ligne**

**Plan de leçon pour les parents ou tuteurs**

Le concept de « vérité » n’a jamais été aussi obscur qu’il ne l’est aujourd’hui. Avant la popularisation d’Internet, les gens consommaient les actualités auprès des médias grand public qui, pour la plupart, étaient réputés pour leurs reportages crédibles et honnêtes. De nos jours, les gens ont la capacité de créer et de partager facilement du contenu, ce qui augmente le potentiel de partage de contenu faux ou trompeur qui ne repose pas sur de l’information réelle, ou qui peut être biaisé.

Lors de la leçon d’aujourd’hui, les élèves apprendront comment évaluer de façon critique ce qu’elles ou ils consomment sur Internet et dans les médias, pour ainsi vérifier si l’information est vraie.

|  |  |
| --- | --- |
| **Accroche**  10 minutes | *Accueillir les élèves*  *Excellente occasion de faire le point sur le bien-être*  *Mettre à profit les connaissances antérieures, rappel de la leçon précédente*  Avant d’entreprendre toute recherche en ligne sur le sujet choisi pour leur infographie sur la citoyenneté numérique (tâche sommative de la leçon 6), les élèves apprendront comment consommer de l’information et comment déterminer si l’information est vraie ou non.  Vos élèves ont-ils déjà entendu l’expression « fausse nouvelle »? Dans le cas contraire, mener une discussion en classe et vérifier ce qu’elles et ils savent déjà à propos des fausses nouvelles, de la propagation de mensonges en ligne et de l’importance de vérifier que ce que l’on voit, entend ou lit en ligne est réellement vrai.  **Exemple de sujet de conversation :**  Il est souvent difficile de déterminer pourquoi les gens mentent en ligne. Souvent, leur but est de provoquer une sorte de réaction, comme la colère ou l’enthousiasme.  Parfois, les gens qui mentent en ligne ont pour but de changer les croyances des gens sur un certain sujet ou de gagner de l’argent en vendant un produit ou une idée (comme la désinformation des sociétés publicitaires). Autrement, parfois les gens font simplement des erreurs - des auteurs, des blogueurs ou des journalistes peuvent avoir oublié de vérifier les faits ou avoir cru honnêtement qu’ils avaient la bonne information.  **Types de mensonges en ligne et exemples d’explications pour les enfants :**   * **Désinformation**: Information en ligne, généralement sous forme d’articles, de vidéos ou de publications sur les médias sociaux qui tentent de faire croire aux enfants qu’ils contiennent des éléments d’information vrais ou factuels, mais qui sont en fait faux et qui visent à répandre des mensonges ou à provoquer une réaction. * **Défis Internet dangereux**: Habituellement, les défis sur Internet encouragent les enfants à faire des choses stupides ou drôles, comme des mouvements de danse ou essayer une sauce piquante; cependant, ces défis peuvent parfois tenter de faire peur aux gens ou même de les amener à se blesser. * **Faux concours en ligne**: Les concours peuvent être très tentants, car ils promettent souvent une sorte de récompense, comme de l’argent ou des objets gratuits pour faire quelque chose d’aussi simple que répondre à une question ou remplir un formulaire. Toutefois, il peut s’agir d’un moyen rapide pour des personnes ou des entreprises inconnues d’obtenir des renseignements personnels ou privés des enfants.   Discuter des exemples d’endroits où des mensonges en ligne peuvent être trouvés. Voici quelques réponses suggérées : jeux en ligne, vidéos, images, actualités, sites Web, médias sociaux, etc. |

|  |  |
| --- | --- |
| **Objectifs d’apprentissage et critères de réussite**  5 minutes | Communiquer les objectifs d’apprentissage pour un apprentissage ciblé. Les critères de réussite renseignent les élèves sur ce qu’elles et ils seront en mesure de faire une fois la matière apprise.  **Objectifs d’apprentissage** :   * Je peux utiliser la pensée critique pour reconnaître les mensonges en ligne ou la fausse information qui est présentée dans les médias. |
| **Données et modélisation** | Enseigner et montrer le contenu et les compétences que les élèves doivent connaître pour réussir. Faire une modélisation à l’aide d’exemples qui éclairent la compréhension.  *Inscrire ici les remarques à l’attention de la Gestion des locaux (matériel supplémentaire).*   * Contenu * *Processus* * *Environnement d’apprentissage* * *Produit*   Avec le document comme guide, passer en revue les catégories courantes de mensonges en ligne que les élèves peuvent rencontrer en parcourant Internet, en regardant leurs vidéos préférées sur YouTube ou en jouant à un jeu sur leur tablette.  Expliquer qu’Internet est un endroit illimité qui s’agrandit littéralement chaque jour. Cet espace est rempli de renseignements et de ressources, c’est pourquoi la capacité de mener une recherche en ligne efficace est une compétence très précieuse.  Encourager les enfants à être des détectives en ligne! Il peut être difficile pour les enfants de faire la différence entre la vérité et les mensonges en ligne, alors il est normal qu’elles et ils demandent un peu d’aide! Suggérer aux enfants de se poser les questions suivantes à propos de ce qu’elles et ils rencontrent en ligne :   * Est-ce trop beau, ou trop laid, pour être vrai? * Le message renferme-t-il des méchancetés à propos de personnes ou de groupes de personnes? * Est-ce étrange, effrayant ou répugnant? * As-tu déjà entendu cette information d’une autre source? Tes amis en ont-ils parlé? As-tu appris cela à l’école? S’agit-il seulement d’une rumeur? * Peux-tu trouver cette information ailleurs sur Internet? L’as-tu vue ailleurs hors ligne, à la télévision ou à la radio, par exemple?   **Remarque importante : Rappeler aux élèves que si elles et ils doutent que quelque chose en ligne soit vrai ou faux, ils devraient le montrer immédiatement à un parent, à une tutrice ou un tuteur ou à une ou un adulte de confiance.** |
| **Pratique guidée et autonome**  20 minutes | *Observer, inviter, soutenir, enrichir*  Une fois que les élèves ont passé en revue les documents et les principales questions de réflexion critique à se poser lorsqu’elles ou ils découvrent de l’information en ligne, leur demander de trouver un article et de déterminer s’il est crédible ou faux.  L’article doit être en lien avec les thèmes abordés jusqu’à maintenant :  1. Cyberrespect et bienveillance en ligne (cyberintimidation)  2. Empreinte numérique positive  3. La communication sécuritaire en ligne  4. Mots de passe et codes d’accès  5. La vérité en ligne  **Renforcement facultatif** : Vous pouvez fournir aux jeunes enfants quelques outils pour les aider à devenir des détectives en ligne et à « décoder » ce qu’ils lisent et regardent en ligne, comme les moteurs de recherche adaptés aux enfants. [Kiddle.co](https://www.kiddle.co/) est un moteur de recherche et une encyclopédie en ligne qui met l’accent sur la sécurité pour les jeunes enfants (en anglais seulement). Encourager les enfants à utiliser Kiddle les aidera à éviter de voir du contenu inapproprié dans leurs résultats de recherche. Il s’agit également d’un bon outil pour les aider à vérifier l’information qu’ils trouvent ailleurs. |
| **Vérification de la compréhension**  10 minutes | *Observations, évaluation formative*  Demander aux élèves de présenter leur article et leurs raisons de croire qu’il est crédible ou faux, en petits groupes. |
| **Conclusion** | *Révision, conclusion, discussion et appréciations* |
| **Ressources** | Ressources pour l’éducateur ou l’éducatrice |
| **Évaluation** | Pour l’apprentissage :   * Observation ✔ * Notes anecdotiques * Liste de vérification * Entretiens et conversations ✔ * Exemples de travaux/produits ✔ * Suivi   En tant qu’apprentissage :   * Rubrique * Critères de réussite ✔ * Introspection * Autre   De l’apprentissage :   * Jeu-questionnaire * Examen * Présentation * Affectation * Autre produit |
| Remarques : |  |

**Leçon 6 : Infographie sur la citoyenneté numérique**

**Plan de leçon pour les parents ou tuteurs**

Aujourd’hui, les élèves vont créer une infographie (représentation visuelle médiatique de l’information), destinée à informer un public sur un thème lié à la cybersécurité dont il a été question dans la documentation vue jusqu’à présent.

Les élèves choisiront l’un des thèmes suivants, qui se rapporte à la citoyenneté numérique, dont traite cette unité, pour leur infographie : cyberrespect et bienveillance en ligne, empreinte numérique positive, communication en ligne sécuritaire, mots de passe et codes d’accès, ainsi que la vérité en ligne.

|  |  |
| --- | --- |
| **Accroche**  10 minutes | *Accueillir les élèves*  *Excellente occasion de faire le point sur le bien-être*  *Mettre à contribution les connaissances antérieures* |
| **Objectifs d’apprentissage et critères de réussite**  5 minutes | Communiquer les objectifs d’apprentissage pour un apprentissage ciblé. Les critères de réussite renseignent les élèves sur ce qu’elles et ils seront en mesure de faire une fois la matière apprise.  **Objectifs d’apprentissage :**   * Je peux créer une infographie (représentation visuelle de l’information) sur un thème lié à la cybersécurité. * Ma représentation graphique communique un argument ou un thème clair lié à la cybersécurité. * Ma présentation visuelle attire l’attention. |
| **Données et modélisation** | Faire l’introduction à l’infographie en partageant des infographies pertinentes que les élèves sont susceptibles de connaître. Il y a probablement des infographies partout dans l’école que vous pouvez utiliser comme exemples! Les infographies sont un moyen spécial d’utiliser les médias numériques pour partager un message ou un thème principal sur un sujet de la cybersécurité. Les élèves devront choisir un thème qui leur importe et créer un message central lié à la citoyenneté numérique pour leur infographie.  Des exemples d’infographies sur la cybersécurité sont disponibles sur le site Web du gouvernement du Canada : <https://www.pensezcybersecurite.gc.ca/fr/ressources>  Exemple d’infographie :    Infographie complète disponible ici :  [*https://www.getcybersafe.gc.ca/en/resources/we-heard-you-got-new-device*](https://www.getcybersafe.gc.ca/en/resources/we-heard-you-got-new-device) |
| **Pratique guidée et autonome**  20 minutes | *Observer, inviter, soutenir, enrichir*  Sur la base des thèmes suivants, les élèves créeront une infographie qui comporte un message central. Les élèves doivent mener des recherches sur ce thème et inclure l’information trouvée dans l’infographie. *(Les thèmes : Cyberrespect et bienveillance en ligne, Empreinte numérique positive, Communication en ligne sécuritaire, Mots de passe et codes d’accès, La vérité en ligne)*  Diriger une séance de remue-méninges pour tous les élèves, puis leur proposer de faire un autre remue-méninges individuellement ou en petits groupes sur des sujets potentiels pour leur infographie *(c.-à-d. comment repérer un cyberintimidateur ou comment créer des mots de passe forts et sécurisés).* |
| **Vérification de la compréhension**  10 minutes | *Observations, évaluation formative*  Une fois que les élèves ont fait un remue-méninges sur des sujets potentiels, élaborer des critères de réussite pour l’infographie.  **Critères de réussite suggérés ou critères de réussite pour commencer** **:**   * Je peux créer une infographie (représentation visuelle de l’information) sur un thème lié à la cybersécurité. * Ma représentation graphique communique un argument ou un thème clair lié à la cybersécurité. * Ma présentation visuelle attire l’attention. |
| **Conclusion** | *Révision, conclusion, discussion et appréciations*  Choisir le sujet : Les élèves peuvent faire part du sujet qu’elles ou ils ont choisi à leur enseignante ou enseignant avant la fin de la période de classe ou avant la leçon suivante.  À l’aide de la rubrique et des critères de réussite, confier la tâche de l’infographie et donnez aux élèves une date d’échéance. |

|  |  |
| --- | --- |
| **Ressources** | Ressources pour l’éducateur ou l’éducatrice  Rubrique (peut être modifiée) |
| **Évaluation** | Pour l’apprentissage :   * Observation✔ * Notes anecdotiques * Liste de vérification * Entretiens et conversations * Exemples de travaux/produits * Suivis   En tant qu’apprentissage :   * Rubrique * Critères de réussite✔ * Introspection * Autre   De l’apprentissage :   * Jeu-questionnaire * Examen * Présentation * Affectation * Autre produit |
| Remarques : |  |