PLAN DE LEÇON

À VOS BOUCLIERS POUR LA CYBERSÉCURITÉ

Cette leçon fait partie de *Utiliser, comprendre et mobiliser : Un cadre de littératie média numérique pour les écoles canadiennes*.

A PROPOS DE L'AUTEUR : Matthew Johnson, Directeur de l'éducation, HabiloMédias

ANNÉES SCOLAIRE : 7e à 9e année

DURÉE : 45 à 60 minutes

Avis de non-responsabilité : CIRA apporte son soutien financier à HabiloMédias. Cette ressource a été élaborée conjointement par CIRA et HabiloMédias. HabiloMédias ne recommande aucune entité commerciale, produit ou service.

Aperçu

Dans cette leçon, les élèves découvrent le concept de défense à double bouclier en matière de cybersécurité :

1. Le bouclier extérieur (défenses techniques périmétriques) : des protections automatiques et structurelles qui empêchent les risques d'atteindre le compte ou l'appareil d'une personne. Il comprend des outils de filtrage DNS (système de noms de domaine), comme le Bouclier canadien de CIRA, des bloqueurs de publicité, l'authentification multifacteur (AMF) et les protections contre le vol intégrées aux appareils.
2. Le bouclier intérieur (vérification cognitive humaine) : des réflexes mentaux qui permettent de repérer, d'analyser et de neutraliser les arnaques qui ont franchi le bouclier extérieur. Il s'agit notamment de détecter les déclencheurs psychologiques (urgence, peur, autorité, secret), d'appliquer la règle « Prends cinq minutes, parles-en à deux personnes » et d'utiliser des méthodes rigoureuses de vérification hors ligne.

Résultats d'apprentissage

Thèmes du cadre : les élèves connaîtront :

- Vie privée et sécurité :
  - Les outils du bouclier extérieur : le fonctionnement du Bouclier canadien de CIRA (filtrage au niveau du DNS), de l'authentification multifacteur (AMF), des bloqueurs de publicité et de scripts intégrés au navigateur ainsi que des protections matérielles et logicielles contre le vol.
  - Les signaux d'alarme du bouclier intérieur : les déclencheurs émotionnels qu'emploient les fraudeurs : l'urgence, la peur ou la panique, la fausse autorité ainsi que le secret ou l'isolement.
  - Les méthodes de vérification essentielles : la règle de prudence « Prends cinq minutes, parles-en à deux personnes », la saisie directe des adresses URL et leur ajout aux favoris, l'utilisation d'un code secret familial pour déjouer les clones vocaux et le « test du

signe de la main en direct » pour détecter les hypertrucages vidéo en temps réel.

Concepts clés : les élèves comprendront que :

- Les médias numériques sont en réseau : se protéger activement en ligne est un geste d'autonomie qui empêche les développeurs sans scrupules, les courtiers en données et les personnes malveillantes de manipuler nos choix, nos finances et nos données.
- Les expériences des médias numériques sont façonnées par les outils que nous utilisons : les boucliers techniques sont essentiels pour bloquer le flot de menaces automatisées, mais l'esprit critique demeure la meilleure défense lorsque des menaces sophistiquées se dissimulent derrière des services réels et dignes de confiance.
- Les interactions sur les médias numériques peuvent avoir une réelle incidence : les fraudeurs sont organisés, agissent à grande échelle et s'appuient sur des techniques avancées de psychologie comportementale pour déjouer nos instincts. Être la cible d'une arnaque, c'est être victime d'une manipulation criminelle; en parler ouvertement et la signaler est un signe de force.

Compétences fondamentales : les élèves seront capables de :

- Accéder : associer et combiner les réglages du bouclier extérieur et les réflexes du bouclier intérieur pour neutraliser des risques numériques complexes qui ciblent les jeunes.
- Utiliser : concevoir un « plan de défense à double bouclier » qui protège le périmètre de leurs appareils et de leurs comptes tout en renforçant leurs réflexes de vérification.
- Comprendre : décortiquer des communications numériques pour repérer le moment précis où le bouclier extérieur a été contourné et celui où le bouclier intérieur doit prendre le relais.

Préparation et matériel pédagogique

Préparez-vous à distribuer les documents *La défense à double bouclier* et *Ordre de mission : deviens responsable de la cybersécurité de ton foyer* ainsi que la fiche d'activité *Conçois ta propre défense à double bouclier*.

Si vous réalisez la démonstration en direct (facultative), préparez-vous à projeter l'écran de votre ordinateur (ou d'un ordinateur de l'école) sur

l'écran ou le tableau blanc interactif, et assurez-vous de pouvoir accéder aux paramètres DNS (système de noms de domaine) et de les modifier.

Imprimez et découpez suffisamment d'exemplaires des cartes d'analyse des menaces (cartes Scénario, cartes Bouclier extérieur et cartes Bouclier intérieur) pour que chaque groupe de 3 ou 4 élèves en ait un exemplaire de chaque.

Déroulement

LE FANTÔME DANS LA BOÎTE DE RÉCEPTION

Commencez par lire le texte suivant aux élèves :

> Imaginez que vous consultez l'un de vos appareils numériques et que vous recevez un message provenant d'un service auquel vous êtes abonnés. L'adresse de l'expéditeur semble correcte et votre service de courriel indique que le message est « sûr » au moyen de coches vertes. Le message annonce que votre compte est sur le point d'être fermé et vous invite à cliquer sur un lien pour empêcher sa fermeture.
>
> Prenez 45 secondes pour noter tout ce qui, dans ce message, pourrait vous sembler suspect.

Accordez ensuite 45 secondes aux élèves pour noter les indices qu'ils ont repérés.

Faites un tour de classe rapide. Chaque élève nomme un indice (p. ex. « l'urgence », « la panique », « un lien sur lequel cliquer »).

Une fois que les élèves ont terminé, expliquez-leur que, pour se protéger contre les arnaques, les logiciels malveillants et les autres cybermenaces, il faut se doter de deux « boucliers » : un bouclier extérieur, composé d'outils de sécurité qui bloquent les menaces avant qu'elles ne nous atteignent et nous empêchent d'accéder à des sites dangereux; et un bouclier intérieur, composé de réflexes mentaux qui nous permettent de repérer les arnaques ne contenant ni fichier ni lien malveillant.

Dites aux élèves :

> « Si vous avez repéré ces indices, c'est que vous étiez déjà à l'affût d'une tromperie. Aujourd'hui, nous allons apprendre à passer du soupçon à l'action en construisant une défense à double bouclier.

Vous aurez ainsi tous les réglages techniques et tous les réflexes nécessaires pour garder le contrôle de vos données et de vos appareils. »

LA DÉFENSE À DOUBLE BOUCLIER

Expliquez maintenant aux élèves que vous allez leur donner des exemples de moyens de se protéger et qu'ils devront indiquer s'il s'agit d'un « bouclier extérieur » (un outil qui tient le danger à distance) ou d'un « bouclier intérieur » (un réflexe ou une idée qui aide à reconnaître et à gérer un risque).

Expliquez qu'à chaque exemple, ils doivent croiser les bras s'il s'agit d'un bouclier extérieur ou se toucher les tempes s'il s'agit d'un bouclier intérieur.

Lisez maintenant les énoncés suivants. Gardez un rythme soutenu et passez au suivant dès que toute la classe a choisi son geste et que vous avez donné votre rétroaction.

- Une serrure à pêne dormant sur la porte d'entrée. (Bouclier extérieur : les élèves doivent croiser les bras.)
- Demander « Qui est là? » quand quelqu'un frappe à la porte. (Bouclier intérieur : les élèves doivent se toucher les tempes.)
- Lire les ingrédients sur un emballage alimentaire pour vérifier qu'il ne contient rien auquel on est allergique. (Bouclier intérieur)
- Une haute clôture de sécurité autour d'une salle de concert. (Bouclier extérieur)

Demandez aux élèves de proposer un autre exemple d'outil qui sert de bouclier extérieur et un autre exemple de réflexe ou d'idée qui sert de bouclier intérieur.

Annoncez-leur ensuite que vous allez leur donner quelques exemples de moyens de se protéger contre les cyberrisques, eux et leurs appareils. Comme tout à l'heure, ils doivent croiser les bras s'ils pensent que l'exemple fait partie du bouclier extérieur, ou se toucher les tempes s'ils pensent qu'il fait partie du bouclier intérieur.

- Utiliser le Bouclier canadien de CIRA sur son routeur, son navigateur ou son appareil. (Bouclier extérieur : le Bouclier canadien bloque les domaines associés aux logiciels malveillants et à l'hameçonnage. Il

empêche donc d'ouvrir un site dangereux ou de suivre un lien qui y mène.)

- Attendre cinq minutes avant de réagir à un message. (Bouclier intérieur : les fraudeurs cherchent à nous faire peur ou à nous bouleverser. Il faut donc toujours prendre le temps de se calmer avant de faire quoi que ce soit.)
- Choisir un code secret familial permettant de vérifier l'identité d'une personne lors d'un appel d'urgence. (Bouclier intérieur : c'est un moyen de vérifier que la personne est bien celle qu'elle prétend être, et non un clone vocal ou un hypertrucage créé par l'IA.)
- Installer un bloqueur de publicité sur son navigateur ou son appareil. (Bouclier extérieur : les bloqueurs de publicité empêchent l'affichage de publicités potentiellement malveillantes et limitent les données que les applications et les sites Web peuvent recueillir.)
- Activer l'authentification multifacteur. (Bouclier extérieur : quand une deuxième étape est exigée pour accéder à nos comptes, comme un code de vérification ou une reconnaissance faciale ou digitale, les pirates ne peuvent pas y accéder même s'ils ont obtenu notre mot de passe à la suite d'une fuite de données.)

Enfin, posez les questions suivantes aux élèves. Ils doivent lever le pouce s'ils pensent que la réponse est « oui » et le baisser s'ils pensent que la réponse est « non ».

- « Si j'installe le Bouclier canadien de CIRA sur mon téléphone, dois-je quand même réfléchir avant d'ouvrir un site Web? » (Pouce levé : le bouclier extérieur et le bouclier intérieur doivent travailler ensemble. Le Bouclier canadien bloque les menaces connues, mais vous devez tout de même vous demander si vous pouvez cliquer sur un lien en toute sécurité.)
- « Si vos parents ou vos tuteurs reçoivent un appel d'une personne dont la voix ressemble à la vôtre, un outil antimaliciel peut-il bloquer cette arnaque? » (Pouce baissé : même sur un téléphone intelligent, le bouclier extérieur ne protège pas contre les arnaques qui misent sur la tromperie et les émotions.)

FACULTATIF : DÉMONSTRATION EN DIRECT

Félicitez les élèves pour l'activité de classement et annoncez-leur que vous allez leur montrer comment activer l'un des outils qu'on règle une fois pour toutes : le Bouclier canadien de CIRA.

Projetez l'écran de votre ordinateur ou de votre tablette au tableau et commentez les étapes suivantes :

« Voyons en 60 secondes comment on active concrètement l'un de nos boucliers extérieurs. Nous allons prendre l'exemple du Bouclier canadien de CIRA. Vous allez voir, c'est tout simple :

1. *D'abord, j'ouvre les paramètres de mon navigateur et je cherche "DNS sécurisé" ou "DNS privé".*
2. *Ensuite, au lieu d'utiliser le fournisseur réseau par défaut, je sélectionne "Personnalisé" et je choisis le Bouclier canadien de CIRA, ou je colle l'adresse de son serveur : private.canadianshield.cira.ca.*
3. *Et voilà! Chaque fois que l'appareil demande l'accès à une page Web, le Bouclier canadien vérifie le domaine à la source afin de s'assurer qu'il ne s'agit pas d'un site d'arnaque ou d'hameçonnage connu. »*

« Faisons maintenant un autre "pouce levé, pouce baissé". Est-ce que je dois prendre une décision ou cliquer sur "Oui" pour chacun des sites Web que je visite? » (Pouce baissé.)

« Non! C'est justement ce qui caractérise les boucliers extérieurs : on les configure une fois, puis on n'a plus à s'en occuper. Ils fonctionnent automatiquement en arrière-plan pour bloquer les contenus indésirables et les liens dangereux avant qu'ils n'atteignent votre appareil. »

LA DÉFENSE À DOUBLE BOUCLIER

Distribuez le document La défense à double bouclier, puis lisez le scénario suivant aux élèves :

> Un fraudeur veut voler l'argent de votre compte de jeu. Il vous envoie un paiement d'un cent par l'intermédiaire de la véritable plateforme PayPal. Dans la note accompagnant le paiement, il écrit : « URGENT : Débit de 987,90 $ en attente. Suivez ce lien ou appelez immédiatement pour l'annuler! »

Demandez aux élèves de réfléchir à la façon dont les boucliers extérieur et intérieur pourraient les protéger. Dites-leur ensuite que vous allez raisonner à voix haute :

Notre bouclier extérieur examine le courriel. Comme il provient du serveur légitime service@paypal.com, il arrive dans notre boîte de réception plutôt que dans le dossier des courriels indésirables. Le Bouclier canadien de CIRA nous empêchera d'ouvrir les liens déjà reconnus comme dangereux. En revanche, c'est notre bouclier intérieur qui nous évitera d'appeler le numéro indiqué et de tomber dans le piège. Nous repérons deux signaux d'alarme : l'urgence (« immédiatement ») et la peur (« débit de 987,90 $ »). Nous appliquons alors la règle « Prends cinq minutes, parles-en à deux personnes ». Après avoir pris du recul et montré le courriel à deux personnes de confiance, nous savons qu'il ne faut pas appeler le numéro indiqué. Nous ouvrons plutôt un nouvel onglet, saisissons nous-mêmes l'adresse paypal.com, puis nous nous connectons à notre compte de façon sécurisée. Nous constatons alors qu'aucun débit de ce montant n'y figure.

ANALYSE DES MENACES

Mise en place : formez des équipes de 3 ou 4 élèves et remettez à chaque groupe un jeu de cartes *Scénario de risque, Outil du bouclier extérieur* et *Action du bouclier intérieur*.

Pour chacun des quatre scénarios de risque, les groupes doivent déterminer ensemble :

1. Quel outil du bouclier extérieur préviendra ou atténuera le mieux la menace au niveau du périmètre.
2. Quelle action du bouclier intérieur les protégera le mieux si la menace franchit le périmètre ou les cible directement.

Soulignez que certaines cartes Bouclier pourraient être utiles dans plus d'un scénario, mais qu'une seule correspond le mieux à chaque scénario.

Chaque groupe doit ensuite rédiger une brève justification de 10 mots expliquant comment les deux niveaux fonctionnent ensemble pour le protéger.

Lorsque les groupes ont terminé, discutez en classe de chaque scénario et des « boucliers » appropriés :

CARTE SCÉNARIO DE RISQUE	BONNE CARTE BOUCLIER EXTÉRIEUR	BONNE CARTE BOUCLIER INTÉRIEUR	PRINCIPE DE DÉFENSE
Le piège de l'abonnement Pendant que tu navigues sur le Web, tu vois une publicité sur un réseau social qui t'annonce que tu as été sélectionné pour gagner un nouveau téléphone, mais l'offre n'est valable que 60 secondes. Si tu cliques sur le lien, il tentera de télécharger un logiciel malveillant sur ton appareil.	*Bouclier canadien de CIRA* Il bloque les domaines liés aux logiciels malveillants, à l'hameçonnage et aux redirections frauduleuses au niveau du DNS, avant même que la connexion soit établie.	*Repère les signaux d'alarme* Méfie-toi des quatre tactiques que les fraudeurs utilisent pour t'empêcher de réfléchir clairement : l'urgence, la peur, l'autorité et le secret.	Le Bouclier canadien empêche tes appareils d'accéder à un site malveillant. L'urgence, comme une offre valable seulement 60 secondes, est l'un des quatre signaux d'alarme d'une arnaque.

Le PDF piégé Tu cherches « skins Fortnite gratuits » et tu vois ce qui ressemble à un résultat commandité. Quand tu cliques dessus, on te demande de télécharger un « guide de trucs et astuces en PDF » pour débloquer ta récompense. Le PDF contient un virus qui infectera ton appareil.	*Outils antimaliciels* Les pare-feux et les outils antimaliciels installés sur ton appareil le protègent contre les logiciels malveillants, comme les virus, que tu pourrais télécharger dans des fichiers ou des pièces jointes.	*On n'a rien pour rien* Une offre te semble trop belle pour être vraie? C'est probablement le cas.	Les outils antimaliciels aident à protéger ton appareil contre les virus cachés dans les fichiers. Et recevoir gratuitement ce que tu voulais? C'est vraiment trop beau pour être vrai!
Le compte piraté Tu reçois un message qui t'annonce que ton compte de réseau social a été piraté et que tu n'y as plus accès. La personne menace de supprimer ton compte si tu ne la paies pas d'ici la fin de la journée.	*Authentification multifacteur* Active l'AMF pour que toute tentative de connexion à partir d'un nouvel appareil exige un texto, une empreinte digitale ou un code généré par une application.	*« Prends cinq minutes, parles-en à deux personnes »* Prends cinq minutes pour respirer. Parles-en à des adultes de confiance qui t'aideront à trouver une solution.	L'authentification multifacteur rend l'accès à tes comptes beaucoup plus difficile, même pour quelqu'un qui connaît ton mot de passe. Prendre le temps de respirer t'aide à faire de meilleurs choix, et des adultes de confiance peuvent t'aider à trouver une solution.

La fuite de mots de passe Une fuite de données sur un site de jeu populaire expose des millions de comptes. Comme tu utilises le même mot de passe pour ton courriel, ton compte Discord et tes comptes scolaires, ils sont tous vulnérables.	*Gestionnaire de mots de passe* Utilise un gestionnaire de mots de passe pour créer des mots de passe robustes et uniques pour tous tes comptes compromis.	*Sécurise et change* Si l'un de tes comptes a été compromis, ne panique pas et ne t'en veux pas. Signale-le au service concerné, puis change le mot de passe de ce compte et de tous les autres comptes qui pourraient être touchés.	Les gestionnaires de mots de passe empêchent qu'un seul mot de passe volé donne accès à plusieurs comptes. Signaler une fuite et changer son mot de passe limite les dégâts.

Faites remarquer aux élèves que, dans certains cas, le bouclier intérieur peut leur éviter d'avoir recours au bouclier extérieur. Par exemple, s'ils reconnaissent que les « skins Fortnite gratuits » sont trop beaux pour être vrais, ils ne téléchargeront pas le fichier. Ils n'auront donc pas besoin d'outils antimaliciels pour protéger leur appareil contre le logiciel malveillant qu'il contient.

VÉRIFICATION DE LA COMPRÉHENSION

Après la discussion, posez la question suivante aux élèves pour vérifier s'ils ont bien compris le fonctionnement des boucliers extérieur et intérieur :

> « Imaginez que vous venez de configurer le Bouclier canadien de CIRA sur votre appareil. Vous recevez un message prétendant provenir de Postes Canada et indiquant que vous devez payer des frais de douane de 2,50 $ pour recevoir un colis. Le message contient un lien pour payer ces frais et obtenir votre colis.
>
> Laquelle des affirmations suivantes est exacte? »

- **Option 1 :** « Si vous suivez le lien, le Bouclier canadien de CIRA bloquera la connexion au niveau du DNS s'il s'agit d'un domaine frauduleux connu. » (**Bonne réponse**)

- **Option 2 :** « Comme vous avez installé le Bouclier canadien de CIRA, un faux texto serait automatiquement supprimé avant même de vous parvenir. Vous pouvez donc cliquer sur n'importe quoi sans danger. » (**Mauvaise réponse** : le Bouclier canadien est un filtre Web qui agit au niveau du DNS. Il ne filtre pas les courriels ni les textos.)
- **Option 3 :** « Le Bouclier canadien de CIRA chiffrera automatiquement vos renseignements de paiement dès que vous les saisirez sur la page de paiement des frais de douane, ce qui protégera votre argent. » (**Mauvaise réponse** : un filtre Web qui agit au niveau du DNS, comme le Bouclier canadien, vous empêche de consulter une page Web malveillante, mais il ne chiffre pas les données que vous transmettez sur une page légitime.)

Demandez aux élèves de lever un doigt pour l'option 1, deux doigts pour l'option 2 ou trois doigts pour l'option 3. Ils peuvent aussi écrire leur réponse sur un petit tableau blanc et la montrer.

Si au moins les trois quarts de la classe choisissent la bonne réponse (option 1), passez à l'étape suivante.

Si moins des trois quarts des élèves choisissent l'option 1, utilisez l'analogie de la porte intelligente pour clarifier :

> « Imaginez que votre école ait une "porte intelligente" qui s'ouvre seulement pour les élèves, les enseignants et le personnel de l'école.
>
> Elle n'empêcherait pas d'autres élèves de vous embêter, et elle ne servirait à rien si vous faisiez entrer quelqu'un avec vous. Par contre, elle garantirait qu'aucune personne étrangère à l'école ne puisse ouvrir la porte.
>
> C'est comme ça que fonctionne un filtre DNS. Il bloque la connexion aux domaines malveillants, mais vous pourriez quand même attraper un logiciel malveillant en téléchargeant un fichier (comme si vous faisiez entrer la mauvaise personne) et vous pourriez quand même vous faire arnaquer par quelqu'un qui utilise un service de paiement légitime. »

DÉFENSE À DOUBLE BOUCLIER PERSONNALISÉE

Distribuez la fiche d'activité Conçois *ta propre défense à double bouclier*.

Demandez à chaque élève de remplir la colonne de gauche (« Configuration de mon bouclier extérieur ») et la colonne de droite (« Les réflexes de mon bouclier intérieur ») avec des actions concrètes. Ces actions doivent s'appuyer sur ce qu'ils ont appris tout en étant adaptées à leurs propres activités et appareils. Par exemple, les élèves qui n'ont pas d'appareil mobile devraient choisir des outils du bouclier extérieur pour les appareils auxquels ils ont accès, comme un ordinateur portable ou une console de jeux. Ceux qui jouent à des jeux vidéo en ligne ou qui font d'autres activités en ligne, comme la programmation, devraient appliquer les conseils et les réflexes du bouclier intérieur aux risques qu'ils pourraient rencontrer dans ces activités.

Si vous le souhaitez, vous pouvez donner aux élèves du temps pour chercher des stratégies et des outils plus précis.

Voici quelques exemples de réponses appropriées :

1. Configuration de mon bouclier extérieur (à régler une fois pour toutes – 2 actions)

Choisis deux réglages techniques qui protègent le périmètre de ton appareil sans te compliquer la vie au quotidien.

- Exemple A : installer le Bouclier canadien de CIRA sur mon téléphone ou mon navigateur pour bloquer les domaines frauduleux au niveau du DNS.
- Exemple B : installer un bloqueur de publicité, comme DuckDuckGo, sur mon téléphone ou mon navigateur.
- Exemple C : activer l'authentification multifacteur (AMF) sur mes comptes de jeux vidéo pour empêcher qu'on pirate mes mots de passe par force brute.

2. Les réflexes de mon bouclier intérieur (vérification mentale active – 2 réflexes)

Choisis deux réflexes à mettre en pratique quand un déclencheur émotionnel se présente.

- Exemple A : penser à appliquer la règle « Prends cinq minutes, parles-en à deux personnes » si je reçois un message m'annonçant que mon compte Scratch a été piraté.

- Exemple B : appliquer la règle « Tape l'adresse, ne clique pas, n'appelle pas » quand je fais des recherches en ligne : toujours ouvrir un nouvel onglet pour me connecter directement au site plutôt que de cliquer sur les liens des notifications ou d'appeler les numéros fournis.
- Exemple C : choisir un code secret familial avec mes grands-parents pour vérifier immédiatement tout appel ou message vocal d'urgence.

Demandez aux élèves d'évaluer, sur une échelle de 1 à 5, la confiance qu'ils accordent à leur plan de défense, puis d'expliquer leur note en une phrase.

Enfin, demandez aux élèves d'échanger leur plan avec un partenaire. Chacun vérifie si les outils du bouclier extérieur sont vraiment automatiques (à régler une fois pour toutes) et si les actions du bouclier intérieur sont bien des réflexes mentaux. Ensuite, chaque élève emprunte une idée au bouclier de son partenaire pour améliorer le sien.

RÉFLEXION

Demandez aux élèves de rédiger une courte réflexion à partir des amorces suivantes :

- « Avant, je pensais que la cybersécurité, c'était… »
- « Maintenant, je pense que la cybersécurité, c'est… »

Juste avant la fin du cours, ou si certains élèves terminent plus tôt, invitez-les à réfléchir à la question suivante :

« Maintenant que je sais comment me protéger, moi et mes appareils, contre les cybermenaces, que pourrais-je faire pour aider ma famille à en faire autant? »

Demandez aux élèves de prendre le document *Ordre de mission : deviens responsable de la cybersécurité de ton foyer* en sortant. Si vous le souhaitez, vous pouvez les inviter à faire part de leurs réflexions au début du cours suivant.

CONSOLIDATION

Un jour ou deux après la leçon, demandez aux élèves de répondre par écrit en deux minutes à la question suivante :

Si un fraudeur réussit à franchir mes deux boucliers et que je clique sur un lien malveillant ou que je communique des renseignements personnels, que dois-je faire immédiatement pour corriger la situation sans paniquer?

Passez les réponses en revue avec la classe et soulignez les étapes suivantes :

1. M'arrêter et respirer : prendre conscience que j'ai été manipulé par des professionnels. Il n'y a aucune honte à avoir.
2. Limiter les dégâts sans tarder : changer les mots de passe de mes comptes principaux, lancer une analyse antivirus complète de mon appareil et en parler à un adulte de confiance.
3. Signaler l'incident : bloquer l'expéditeur et faire un signalement officiel au Centre antifraude du Canada pour aider à protéger d'autres jeunes.

DOCUMENT D'ACCOMPAGNEMENT

À VOS BOUCLIERS POUR LA CYBERSÉCURITÉ

LA DÉFENSE À DOUBLE BOUCLIER

Pour te protéger, toi et tes appareils, il te faut **deux boucliers** : un **bouclier extérieur**, qui empêche les menaces de t'atteindre, et un **bouclier intérieur**, qui t'aide à reconnaître les risques que le bouclier extérieur n'a pas arrêtés.

LE BOUCLIER EXTÉRIEUR

Protection automatique du périmètre

Bloque les connexions malveillantes (Bouclier canadien de CIRA)

Quand tu essaies de consulter un site Web, ton appareil demande à un « résolveur DNS » (système de noms de domaine) de traduire l'adresse ou le nom de domaine du site, comme www.cira.ca, en une adresse IP qui permet d'atteindre cette destination. Le Bouclier canadien de CIRA (https://www.cira.ca/fr/canadian-shield/) bloque les logiciels malveillants, les sites d'hameçonnage et les sites frauduleux connus dès cette étape, ce qui empêche toute connexion au site dangereux.

Protège tes appareils contre les logiciels malveillants

Utilise les pare-feux et les outils antimaliciels de tes appareils pour les protéger contre les logiciels malveillants, comme les virus, que tu pourrais télécharger dans des fichiers ou des pièces jointes.

Bloque les publicités et les scripts dangereux (bloqueurs de publicité)

Bloque les scripts publicitaires malveillants (la « publicité malveillante ») et les témoins de suivi qu'utilisent les courtiers en données et les fraudeurs qui veulent te cibler avec des arnaques adaptées à tes intérêts.

Sécurise tes comptes (mots de passe robustes et uniques, et authentification multifacteur)

Utilise des mots de passe d'au moins 8 caractères, qui ne sont pas des mots du dictionnaire et qui ne comportent pas de substitutions faciles à deviner (comme «1» à la place de «l»). Utilise un mot de passe différent pour chaque compte. Ainsi, si le mot de passe d'un compte est exposé lors d'une fuite de données, les pirates ne pourront pas accéder à tes autres comptes. Les gestionnaires de mots de passe facilitent l'utilisation de mots de passe robustes et uniques pour chaque compte.

Exige une deuxième vérification, par reconnaissance biométrique ou par code d'authentification, pour te connecter. Personne ne pourra ainsi accéder à ton compte, même si ton mot de passe a été divulgué lors d'une fuite de données. Active les fonctions de protection contre le vol de ton appareil, comme la protection en cas de vol de l'appareil ou le verrouillage en cas de détection de vol, pour qu'une vérification supplémentaire soit nécessaire avant de modifier les réglages de sécurité importants.

LE BOUCLIER INTÉRIEUR

Réflexes mentaux et émotionnels

Repère les signaux d'alarme (urgence, peur, autorité, secret)

- Les fraudeurs utilisent quatre déclencheurs pour court-circuiter ton esprit critique :
- L'urgence : des messages comme « Agissez dans les 24 prochaines heures! » te poussent à agir immédiatement, sur un coup de tête.
- La peur ou la panique : des avertissements comme « Votre compte sera supprimé définitivement » ou « Un coursier passera chercher l'argent comptant » provoquent une réaction de peur.
- La fausse autorité : en se faisant passer pour des organismes de confiance (police, banques, Agence du revenu du Canada, Netflix, entreprises de jeux vidéo), les fraudeurs t'amènent à baisser ta garde.
- Le secret ou l'isolement : les fraudeurs disent des choses comme « Il s'agit d'une enquête confidentielle. N'en parle pas à tes parents ni à tes amis » pour t'empêcher de parler à d'autres personnes qui pourraient t'aider à comprendre qu'il s'agit d'une arnaque.

Vérifie avant d'agir (« Prends cinq minutes, parles-en à deux personnes »)

Si un message utilise l'un de ces quatre déclencheurs, prends une pause de cinq minutes pour laisser redescendre ton taux d'adrénaline. Ensuite, parles-en à deux personnes différentes (un parent, un enseignant, un ami). Les fraudeurs comptent sur l'isolement, alors raconter ce qui t'arrive à d'autres personnes brise l'illusion. Un « code secret » peut aussi vous aider, ta famille et toi, à vérifier que vous parlez bien à la bonne personne et non à un clone vocal ou à un hypertrucage.

Sache qu'on n'a rien pour rien

Les offres qui semblent trop belles pour être vraies sont un autre signe courant d'arnaque. Il existe de vraies offres, mais vérifie toujours qu'elles proviennent de sources fiables.

Utilise la navigation directe (« Tape l'adresse, ne clique pas, n'appelle pas »)

Ne suis jamais un lien, ne réponds jamais à un message et n'appelle jamais un numéro qui se trouve dans un message utilisant l'un de ces quatre déclencheurs. Trouve toi-même la véritable adresse Web de l'organisme et communique avec lui par ce moyen.

Réagis aux risques de sécurité

Si tu apprends qu'il existe un risque pour toi ou pour tes appareils, règle le problème. Supprime les vieux comptes que tu n'utilises plus et change ton mot de passe si l'un de tes comptes a été compromis.

Pense aux autres

Si toi ou une personne que tu connais êtes victimes d'une arnaque, bloque l'expéditeur et fais un signalement au Centre antifraude du Canada (https://antifraudcentre-centreantifraude.ca/report-signalez-fra.htm) pour éviter que la même chose arrive à d'autres personnes.

DOCUMENT D'ACCOMPAGNEMENT

À VOS BOUCLIERS POUR LA CYBERSÉCURITÉ

Cartes d'analyse des menaces

CARTES SCÉNARIO

Le PDF piégé

Tu cherches « skins Fortnite gratuits » et tu vois ce qui ressemble à un résultat commandité. Quand tu cliques dessus, on te demande de télécharger un « guide de trucs et astuces en PDF » pour débloquer ta récompense. Le PDF contient un virus qui infectera ton appareil.

Le compte piraté

Tu reçois un message qui t'annonce que ton compte de réseau social a été piraté. La personne menace de supprimer ton compte si tu ne la paies pas d'ici la fin de la journée.

La fuite de mots de passe

Une fuite de données sur un site de jeu populaire expose des millions de comptes. Comme tu utilises le même mot de passe pour ton courriel, ton compte Discord et tes comptes scolaires, ils sont tous vulnérables.

Le piège de l'abonnement

Pendant que tu navigues sur le Web, tu vois une publicité sur un réseau social qui t'annonce que tu as été sélectionné pour gagner un nouveau téléphone, mais l'offre n'est valable que 60 secondes. Si tu cliques sur le lien, il tentera de télécharger un logiciel malveillant sur ton appareil.

Cartes Bouclier extérieur

Bouclier canadien de CIRA

Il bloque au niveau du DNS les domaines connus pour être liés aux logiciels malveillants, aux réseaux de zombies, à l'hameçonnage et aux redirections frauduleuses.

Outils antimaliciels

Les pare-feux et les outils antimaliciels installés sur ton appareil le protègent contre les logiciels malveillants, comme les virus, que tu pourrais télécharger dans des fichiers ou des pièces jointes.

Authentification multifacteur

Active l'AMF pour que toute tentative de connexion à partir d'un nouvel appareil exige un texto, une empreinte digitale ou un code généré par une application.

Gestionnaire de mots de passe

Utilise le gestionnaire de mots de passe de ton appareil pour créer des mots de passe robustes et uniques pour tous tes comptes compromis.

Cartes Bouclier intérieur

On n’a rien pour rien

Une offre te semble trop belle pour être vraie? C’est probablement le cas.

« Prends cinq minutes, parles-en à deux personnes »

Prends cinq minutes pour respirer. Parles-en à des adultes de confiance qui t’aideront à trouver une solution.

Sécurise et change

Si l’un de tes comptes a été compromis, ne panique pas et ne t’en veux pas. Signale-le au service concerné, puis change le mot de passe de ce compte et de tous les autres comptes qui pourraient être touchés.

Repère les signaux d’alarme

Méfie-toi des quatre tactiques que les fraudeurs utilisent pour t’empêcher de réfléchir clairement : l’urgence, la peur, l’autorité et le secret.

DOCUMENT D'ACCOMPAGNEMENT

À VOS BOUCLIERS POUR LA CYBERSÉCURITÉ

Conçois ta propre défense à double bouclier

TA MISSION : DEVENIR STRATÈGE DE LA SÉCURITÉ NUMÉRIQUE!

Les fraudeurs et les pirates ont plus d'un tour dans leur sac pour s'infiltrer dans tes appareils, voler tes comptes ou te pousser à révéler des secrets. Mais tu n'es pas une cible : tu es un stratège!

Tu vas créer ta propre stratégie de défense à double bouclier, c'est-à-dire des gestes que tu peux poser dès maintenant pour mieux protéger tes appareils et tes activités en ligne. Tu présenteras ta défense en remplissant un tableau en T tout simple.

ÉTAPE 1 : REMPLIS TON « BOUCLIER EXTÉRIEUR » (COLONNE DE GAUCHE)

Ton bouclier extérieur est formé de réglages techniques automatiques. Tu les configures une seule fois, puis ils fonctionnent en arrière-plan pour bloquer les dangers avant même qu'ils atteignent ton appareil.

Note exactement 2 actions que tu vas mettre en place pour ton bouclier extérieur. Assure-toi qu'elles conviennent aux appareils que tu utilises vraiment, comme un téléphone, un ordinateur portable, une console de jeux, etc.

ÉTAPE 2 : REMPLIS TON « BOUCLIER INTÉRIEUR » (COLONNE DE DROITE)

Aucun outil technique n'est parfait, et il arrive que des arnaques passent à travers ton bouclier extérieur. C'est là que tu actives ton bouclier intérieur : le mode détective de ton cerveau! Et parfois, grâce à ton bouclier intérieur, ton bouclier extérieur n'aura même pas besoin d'intervenir.

Note exactement 2 réflexes que tu vas adopter pour ton bouclier intérieur. Assure-toi qu'ils correspondent à ce que tu fais en ligne, comme jouer à des jeux vidéo, regarder des vidéos, t'informer sur des sujets qui t'intéressent, programmer, etc.

ÉTAPE 3 : ÉCHELLE DE CONFIANCE

Évalue ton degré de confiance dans ta stratégie sur une échelle de 1 à 5 et explique ta note en une phrase.

ÉTAPE 4 : ÉCHANGE DE BOUCLIERS

Échange ton plan avec un partenaire. Demande-lui de vérifier si les éléments de ton bouclier extérieur sont vraiment automatiques (à régler une fois pour toutes) et si ceux de ton bouclier intérieur sont bien des réflexes mentaux. Emprunte ensuite un outil ou un réflexe à son bouclier pour améliorer le tien, et ajoute-le dans la colonne de gauche ou de droite.

Liste de vérification : travail à remettre

Avant de remettre ton tableau en T, vérifie ton travail :

- ☐ Ai-je noté exactement 2 actions précises dans la colonne de mon bouclier extérieur?
- ☐ Ai-je noté exactement 2 réflexes précis dans la colonne de mon bouclier intérieur?
- ☐ Mes choix sont-ils adaptés à mes propres appareils et à ce que j'aime faire en ligne?
- ☐ Ai-je évalué mon degré de confiance dans ma stratégie et expliqué ma note en une phrase?
- ☐ Ai-je échangé mon tableau en T avec un partenaire, donné et reçu des commentaires, et emprunté un de ses outils ou réflexes?

CONFIGURATION DE MON BOUCLIER EXTÉRIEUR À régler une fois pour toutes : 2 actions *Choisis deux outils ou réglages qui te protègent, toi et ton appareil, sans te compliquer la vie.*	Les réflexes de mon bouclier intérieur Réfléchir avant d'agir : 2 réflexes *Choisis deux réflexes à adopter chaque fois qu'une situation te stresse, te bouleverse ou éveille tes soupçons.*

DOCUMENT D'ACCOMPAGNEMENT

À VOS BOUCLIERS POUR LA CYBERSÉCURITÉ

ORDRE DE MISSION : DEVIENS RESPONSABLE DE LA CYBERSÉCURITÉ DE TON FOYER

Maintenant que tu sais utiliser les boucliers extérieur et intérieur pour te protéger, toi et tes appareils, ta mission est d'accompagner ta famille pour que tout le monde soit à l'abri des fraudeurs et des cybermenaces.

MISSION 1 : PROTÉGER TES PARENTS OU TUTEURS (LES FONDATIONS)

Ce sont souvent les parents et les tuteurs qui s'occupent des comptes les plus importants de la famille, comme ceux de la banque et des impôts. Demande-leur s'ils ont mis en place les éléments suivants du bouclier :

BOUCLIER EXTÉRIEUR (À RÉGLER UNE FOIS POUR TOUTES)	BOUCLIER INTÉRIEUR (RÉFLEXES MENTAUX)
Installer le Bouclier canadien de CIRA : demande à tes parents ou tuteurs s'ils l'ont configuré sur le routeur de la maison et sur tous les appareils connectés. Il filtre les connexions au niveau du DNS pour bloquer l'accès aux sites malveillants avant même qu'elles s'établissent.	« Prends cinq minutes, parles-en à deux personnes » : tu as reçu un message inquiétant ou bouleversant? Prends cinq minutes pour te calmer, puis parles-en à deux personnes pour vérifier s'il pourrait s'agir d'une arnaque.
Gestionnaires de mots de passe : ils créent des mots de passe robustes et uniques pour qu'une seule fuite ne compromette pas tous les comptes.	« Tape l'adresse, ne clique pas, n'appelle pas » : ne clique jamais sur les liens contenus dans les messages. Tape toujours la véritable adresse du site dans ton navigateur.
Protection en cas de vol de l'appareil : cette fonction exige une vérification biométrique pour accéder aux réglages sensibles si un téléphone est perdu ou volé.	Vérifie l'état du compte : si un message prétend qu'il y a un problème, connecte-toi directement au vrai site pour vérifier.

MISSION 2 : GUIDER TES FRÈRES ET SŒURS (LE PLAN DE MATCH)

Les frères et sœurs sont souvent ciblés par l'intermédiaire des jeux et des réseaux sociaux. Avec tes parents ou tuteurs, aide-les à construire leur propre bouclier pour protéger leurs tablettes et leurs consoles.

- Bloqueurs de publicité (bouclier extérieur) : ils empêchent les publicités « piégées » et les scripts malveillants de s'afficher sur les sites Web.
- Outils antimaliciels (bouclier extérieur) : ils agissent comme une clôture numérique qui bloque les virus cachés dans les téléchargements « gratuits » ou les pièces jointes.
- Repérer ce qui est trop beau pour être vrai (bouclier intérieur) : apprends à tes frères et sœurs à reconnaître que les offres de skins ou de guides de trucs et astuces « gratuits » pour les jeux sont généralement des pièges pour voler des données.
- La règle d'or : toujours demander à un adulte avant de cliquer sur un lien « gratuit » ou de télécharger un nouveau fichier.

MISSION 3 : SOUTENIR TES GRANDS-PARENTS (LES EXPERTS DE LA VÉRIFICATION)

Les grands-parents sont souvent ciblés par des fraudeurs qui exercent une forte pression et ont recours à l'IA et à la tromperie. Discute avec tes parents ou tuteurs de la façon d'aider tes grands-parents à devenir des experts du bouclier intérieur grâce aux étapes suivantes :

1. Choisir un code secret familial : choisissez un mot précis pour vérifier les appels. Si quelqu'un appelle en prétendant être un membre de la famille en difficulté, cette personne doit connaître le code secret.
2. Repérer les quatre déclencheurs : explique-leur que les fraudeurs utilisent l'urgence (« Agissez maintenant! »), la peur ou la panique (« Vous avez de gros ennuis! »), la fausse autorité (« Je travaille pour le gouvernement! ») et le secret ou l'isolement (« N'en parlez à personne! ») pour empêcher les gens de réfléchir clairement.
3. La règle « Tape l'adresse, ne clique pas » : ne clique jamais sur les liens contenus dans des messages qui prétendent provenir d'une banque, de l'ARC ou de Netflix. Saisis plutôt toi-même l'adresse Web dans le navigateur. Tu peux les aider à enregistrer dans leurs favoris les bonnes adresses de leurs banques, de leurs services de diffusion en continu et de leurs autres services afin qu'ils n'aient pas à les saisir chaque fois.

Grâce à ces deux boucliers, ta maison est maintenant une vraie forteresse de cybersécurité!