



Soyez cyber-chouette !

Enseigner aux élèves du primaire les enjeux de la cybersécurité et de meilleures façons pour se protéger en ligne



Niveau 2



Introduction

Niveau 2



Bienvenue dans le second niveau de ce recueil de six leçons en cybersécurité de Labos Créatifs. Ce guide s'adresse aux personnes enseignantes de la maternelle à la 6^e année. Nous vous proposerons six nouvelles leçons pour vous aider à enseigner les dangers, les pièges et les trucs pour apprendre à se protéger sur internet. Il n'y a personne de mieux placés que vous pour décider de quand et de comment vous intégrerez ces leçons à vos programmes d'études et le temps que vous pourrez y consacrer avec vos élèves selon leur âge et leurs intérêts.

Les six leçons sont tout simplement des supports visuels que vous pourrez utiliser au meilleur moment en classe avec vos élèves. Nous vous suggérerons des pistes de discussion et des idées d'activités pour renforcer ce que vous aurez présenté. Pas besoin d'avoir déjà reçu une formation en cybersécurité ou d'avoir de grandes connaissances dans le domaine. Tout est prêt pour vous ! Le plus important est de prendre du temps en classe avec vos élèves pour en discuter, pour clarifier certains concepts au besoin et pour apprendre des trucs faciles pour mieux se protéger sur le Web. Ce deuxième niveau en cybersécurité comprend les leçons suivantes ;

- *Leçon # 7 ; L'ingénierie sociale est un autre type de piège de la cybersécurité.*
- *Leçon # 8 ; L'internet des objets (Ido) ; il est important de connaître les risques.*
- *Leçon # 9 ; L'intelligence artificielle (IA), il faut faire attention aux hallucinations.*
- *Leçon # 10 ; Les villes intelligentes peuvent offrir des avantages, mais également des risques.*
- *Leçon # 11 ; Il y a beaucoup de métiers à découvrir en cybersécurité.*
- *Leçon # 12 ; Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.*

Le premier niveau comprend les leçons ci-dessous que nous suggérons de faire en premier ;

- *Leçon # 1 ; Il est essentiel d'apprendre à ne pas tomber dans les pièges de la cybersécurité.*
- *Leçon # 2 ; Il faut toujours utiliser un mot de passe robuste.*
- *Leçon # 3 ; L'hameçonnage, ne pas se faire attraper comme un poisson.*
- *Leçon # 4 ; Les malicieux, apprenez ce qu'ils sont et ce qu'ils font.*
- *Leçon # 5 ; Protégeons notre vie privée ; ne soyons pas un livre ouvert.*
- *Leçon # 6 ; Les réseaux sociaux ; il vaut mieux réfléchir pour se protéger.*





Introduction



Évidemment, vous pouvez intégrer ce contenu dans vos cours et de faire des liens avec le vécu des élèves et de leurs familles. Il est important de suivre l'ordre établi pour une plus grande fluidité lorsque vous passerez d'une leçon à une autre. En plus de conseils pour animer les présentations, vous trouverez dans ce recueil des questions d'objectivation, des idées d'activités complémentaires et des sites Web pour aller plus loin que vous pourrez intégrer dans les apprentissages réguliers de vos matières à chaque leçon proposée.

Utilisez les supports visuels des leçons de préférence sur un grand écran, une diapositive à la fois et prenez un moment pour avoir des discussions franches avec vos élèves. **Ici, c'est la qualité et non la quantité qui sera privilégié !**

On entend souvent que la cybersécurité est l'affaire de tous. Les écoles et les personnes enseignantes ont aussi un grand rôle à jouer pour éduquer à propos de la cybersécurité. Nous espérons que vous voudrez bien vous aventurer avec nous dans le monde de la cybersécurité avec vos élèves ! Nous sommes certains que vous apprendrez, vous aussi, plein de nouvelles choses qui pourront vous aider au travail et dans votre vie au quotidien. Encore mieux, ce sont vos élèves qui pourront apprendre des choses essentielles pour apprendre à mieux se protéger en ligne et lorsqu'ils utilisent du matériel informatique ou leurs cellulaires.



17 objectifs de développement durable (ODD) des Nations-Unies

En septembre 2015, les 193 États membres de l'Assemblée générale des Nations Unies ont adopté à l'unanimité la résolution « Transformer notre monde : le Programme de développement durable à l'horizon 2030 ». Aussi connue sous le nom « Programme 2030 », la résolution a établi les **17 objectifs de développement durable** (aussi appelés ODD) qui visent à réaliser le développement durable dans ses dimensions économiques, sociale et environnementale à l'échelle mondiale d'ici à 2030. Les ODD et les 169 cibles connexes visent notamment à éliminer la pauvreté mondiale, à parvenir à l'égalité entre les sexes,



Introduction



à promouvoir la croissance économique, à protéger l'environnement et à créer des institutions efficaces, responsables et transparentes. Chez Labos Créatifs, nous trouvons important de faire des liens entre toutes nos initiatives et les 17 ODD. Avec ce recueil de leçons en cybersécurité, les ODD touchées sont les suivantes ; # 4, 8, 9, 10, 11, 12, 16 & 17.



Nous vous encourageons donc à inclure les 17 ODD dans la planification de toutes vos activités d'apprentissages au quotidien et de faire connaître celles-ci à tous vos élèves ainsi qu'à votre communauté éducative.

Des découvertes passionnantes ont été faites dans le monde de la cybersécurité. Voici donc un excellent sujet à explorer avec vos élèves !

N'hésitez pas à nous faire signe au besoin et à nous transmettre vos découvertes et vos histoires à succès au fils des nouvelles leçons apprises.



Soyez cyber-chouette!

Enseigner aux élèves du primaire les enjeux de la cybersécurité
et de meilleures façons pour se protéger en ligne

Niveau 1



Soyez cyber-chouette!

Leçon # 1

Apprendre à se protéger
pour les élèves du primaire

Ne tombez pas dans les
pièges des cyberpirates.



Soyez cyber-chouette!

Leçon # 2

Apprendre à se protéger
pour les élèves du primaire

Il faut toujours utiliser un
mot de passe robuste.



Soyez cyber-chouette!

Leçon # 3

Apprendre à se protéger
pour les élèves du primaire

L'hameçonnage,
ne pas se faire attraper
comme un poisson.



Soyez cyber-chouette!

Leçon # 4

Apprendre à se protéger
pour les élèves du primaire

Les malicieux, apprenez ce
qu'ils sont et ce qu'ils font.



Soyez cyber-chouette!

Leçon # 5

Apprendre à se protéger
pour les élèves du primaire

Protégeons notre vie privée ;
ne soyons pas un livre ouvert.



Soyez cyber-chouette!

Leçon # 6

Apprendre à se protéger
pour les élèves du primaire

Les réseaux sociaux; Il vaut
mieux réfléchir pour se protéger.



Soyez cyber-chouette!

Enseigner aux élèves du primaire les enjeux de la cybersécurité et de meilleures façons pour se protéger en ligne

Soyez cyber-chouette!

Leçon # 7

Apprendre à se protéger pour les élèves du primaire

L'ingénierie sociale est un autre type de piège de la cybersécurité.

Brilliant LABS Créatifs



Niveau 2



Soyez cyber-chouette!

Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

Brilliant LABS Créatifs



Soyez cyber-chouette!

Leçon # 9

Apprendre à se protéger pour les élèves du primaire

L'intelligence artificielle (IA), il faut faire attention aux hallucinations.

Brilliant LABS Créatifs



Soyez cyber-chouette!

Leçon # 10

Apprendre à se protéger pour les élèves du primaire

Les villes intelligentes peuvent offrir des avantages mais aussi des risques.

Brilliant LABS Créatifs



Soyez cyber-chouette!

Leçon # 11

Apprendre à se protéger pour les élèves du primaire

Il y a beaucoup de métiers à découvrir en cybersécurité!

Brilliant LABS Créatifs



Soyez cyber-chouette!

Leçon # 12

Apprendre à se protéger pour les élèves du primaire

12 conseils à retenir pour devenir cyber-chouette en cybersécurité.

Brilliant LABS Créatifs





Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



Objectif de cette leçon

Dans la leçon # 7, les élèves pourront comprendre ce que c'est l'ingénierie sociale et des moyens pour apprendre à mieux se protéger.

Démarche proposée

Nous vous suggérons tout simplement de prendre un moment dans la journée pour passer en revue les différentes diapositives de la leçon # 7 et d'avoir une discussion avec vos élèves concernant les pièges de la cybersécurité. Il n'est pas nécessaire d'avoir de grandes connaissances dans le domaine. Grâce aux diapositives de la leçon # 7 du programme "**Soyez cyber-chouette !**" comme support pédagogique, vous pourrez facilement présenter de nouveaux concepts et des mots importants ainsi que le jargon du monde de la cybersécurité. L'important ici sera de prendre un temps d'arrêt et d'avoir cette discussion unique et essentielle avec vos élèves.

Questions d'objectivation

Voici quelques exemples de questions d'objectivations qui pourraient être utiles pendant ou après avoir visionné la leçon. N'hésitez pas à les modifier ou à y ajouter vos propres questions au besoin ;

- **Élèves de la maternelle à la 3^e année ;**
 - *Quels sont des pièges que les cyberpirates peuvent utiliser lorsque nous utilisons les appareils branchés à internet ?*
 - *Pourquoi font-ils cela ?*
- **Élèves de 4^e à la 6^e année ;**
 - *On dit souvent que le renard est un animal rusé ? Pourquoi ?*
 - *Est-ce que les cyberpirates peuvent eux aussi être rusés ? Avez-vous des exemples ?*
 - *Qu'est-ce qu'un sentiment d'urgence ? Avez-vous des exemples ?*
 - *Comment est-ce que la fait de ne pas réfléchir avant de faire quelque chose peut-il nous donner des désagréments ?*
 - *Avez-vous des trucs pour prendre les meilleures décisions possibles ?*
 - *Avez-vous appris quelque chose de nouveau aujourd'hui ? Expliquez ?*



Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



Soyez cyber-chouette!

Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS



Diapositive 1 ;

L'objectif de la leçon # 7 est de comprendre ce qu'est l'ingénierie sociale et d'apprendre à bien se protéger et d'expliquer comment ne pas tomber dans les pièges.

Diapositive 2 ;

Prendre un moment pour avoir une discussion pour voir si certains élèves en ont déjà entendu parler et s'ils veulent faire des hypothèses sur ce que ça pourrait être s'ils ne le savent pas.



L'ingénierie sociale, c'est quoi ?

Diapositive 3 ;

L'ingénierie sociale, c'est lorsqu'un cyberpirate utilise des tactiques pour voler des informations personnelles et sensibles. Souvent, ils utilisent la peur ou l'excitation à l'idée de gagner un prix pour qu'une personne agisse rapidement.

L'ingénierie sociale c'est un peu comme faire une enquête.



Diapositive 4 ;

L'ingénierie sociale est une façon malhonnête de nous attraper et de nous faire tomber dans des pièges de la cybersécurité. Elle peut aussi être appelée "le piratage psychologique". Les cyberpirates cherchent des moyens pour nous faire réagir rapidement sans trop réfléchir.

Certains cyberpirates utilisent des tours pour découvrir des choses sur les personnes. Ils essaient de les tromper et de leur prendre leurs informations.



Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS
LABOS



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



Comment est-ce que ça fonctionne ?

Diapositive 5 ;

En général, nous recevons des courriel ou des appels téléphoniques frauduleux. Cela peut même aller jusqu'à ce qu'une personne frappe à notre porte pour nous demander des informations personnelles ou sensibles.

L'ingénierie sociale

Les cyberpirates utilisent plusieurs façons de faire leurs enquêtes. Nous avons déjà discuté dans les autres leçons des exemples suivants :



- L'hameçonnage
- Les maliciels
- L'échange des informations personnelles et sensibles

Source: Terrameca Security

Diapositive 6 ;

Nous avons déjà vu l'hameçonnage (leçon # 3), les maliciels (leçon # 4) et Les informations personnelles et sensibles (leçon # 5). Profitez-en pour faire un rappel de ces leçons.

L'ingénierie sociale

Il y en a d'autres pièges plus ou moins compliqués aussi comme :



- L'appâtage
- L'attaque de point d'eau
- L'hameçonnage vocal
- La prise d'une fausse identité
- Le talonnage

Source: Terrameca Security

Diapositive 7 ;

Les pièges tendus par les cyberpirates peuvent être complexes. Ici, l'important pour les élèves, c'est de voir qu'il en existe plusieurs. Ils n'ont pas à tout retenir. S'ils ont des doutes, il est important d'en discuter avec un adulte.

L'appâtage est un piège utilisé en cybersécurité. On attire les personnes à faire des actions en échange à une récompense comme un film gratuit ou l'accès à un nouveau jeu en ligne.



Source: Terrameca Security

Diapositive 8 ;

Souvent, ce genre de piège propose des concours de toutes sortes, des prix très alléchants et des privilèges comme accéder à des niveaux supérieurs dans des jeux vidéos par exemple.



Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



L'attaque de point d'eau essaie d'attirer des personnes sur un site web vulnérable.

Source: Terranoco Security

Diapositive 9 ;

Les pirates informatiques essaient de vous attirer sur un site web peu sécurisé qui est en fait un espace dans lequel, c'est beaucoup plus facile pour eux d'installer des vulnérabilités sur vos appareils informatiques ou vos cellulaires.


L'hameçonnage vocal est un message qu'on reçoit et qui peut nous faire paniquer et agir rapidement sans trop réfléchir.



Source: Terranoco Security

Diapositive 10 ;

Certains cyberpirates peuvent vous appeler ou vous envoyer un message vocal en prétextant, par exemple, que votre compte bancaire est en danger ou que vous avez été piraté. C'est souvent une urgence.



La prise d'une fausse identité est lorsqu'un pirate se fait passer pour une autre personne afin de nous voler des informations.

Source: Terranoco Security

Diapositive 11 ;

Parfois, certains cyberpirates prennent une fausse identité pour créer un lien de confiance et essayer ainsi de vous voler de fausses informations. Souvent, ils disent qu'ils veulent vous aider.



Le talonnage, c'est une tactique pour accéder physiquement dans un endroit sécurisé sans permission dans le but de voler des renseignements ou du matériel informatique.

Source: Terranoco Security

Diapositive 12 ;

Certains cyberpirates conduisent l'audace jusqu'à se rendre dans des endroits pour accéder à du matériel informatique, pour le voler ou pour y installer des logiciels malicieux. Ils peuvent, par exemple, se faire passer pour un réparateur.



Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS
LABOS



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



C'est pour cela qu'il est super important d'apprendre à bien se protéger !

Diapositive 13 ;

Il est important de marteler le point qu'il est essentiel d'apprendre et de continuer à apprendre au sujet de la cybersécurité. Il y aura d'autres changements au cours des prochaines années, car la cybersécurité évolue elle aussi.

Il est super important d'apprendre à éviter les pièges de l'ingénierie sociale !



Diapositive 14 ;

Les cyberpirates essaient de nous tendre toutes sortes de pièges. On peut les déjouer en étant au courant de ce que sont ces pièges et de comment les éviter.

Des trucs utiles...

- Continuer à apprendre au sujet de la cybersécurité
- Parlez-en avec des adultes et d'autres personnes de votre entourage.
- Si c'est trop beau pour être vrai, ce n'est probablement pas vrai.
- Ne prenez pas de risques inutiles en participant à des concours ou en partageant des informations personnelles et sensibles.



Diapositive 15 ;

L'important ici pour les élèves, est de comprendre qu'utiliser un bon jugement et de demander de l'aide à un adulte de confiance s'ils ne sont pas certains sont de bonnes façons de se protéger.

D'autres trucs utiles...

- Ne cliquez jamais sur des liens louches provenant de courriel bizarres.
- Ne répondez pas à des demandes de toutes sortes.
- Ne visitez pas de sites Web louches ou des sites de publicités inconnus.
- N'acceptez jamais qu'une personne inconnue vienne vous rencontrer.
- Demandez l'aide d'un adulte de confiance en tout temps si vous n'êtes pas certain.

Diapositive 16 ;

Il est très important de faire attention aux endroits que l'on visite sur le Web et sur les réseaux sociaux.



Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS
LABOS



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



Enfin...

- Faites confiance à votre instinct si vous n'êtes pas certain ou si vous avez peur.
- Soyez vigilant en tout temps et méfiez-vous des messages qui promettent des cadeaux, des accès à des jeux ou à des images gratuitement si vous acceptez de cliquer sur un lien ou de donner vos informations personnelles et sensibles.



Diapositive 17 ;

En général, si on a peur ou si on sent qu'il y a quelque chose de louche, c'est souvent qu'il y a un piège. On demande alors à un adulte de confiance de nous aider.

Leçon # 7

L'ingénierie sociale
est un autre type
de piège de la
cybersécurité.



Diapositive 18 ;

C'est l'essentiel de la leçon # 7. Il faut se rappeler que les cyberpirates utilisent aussi toutes sortes de pièges qui font appel à l'ingénierie sociale pour créer un sentiment de peur ou d'urgence afin que nous décidions de faire des mauvais choix.

Soyez
cyber-chouette!



Diapositive 19 ;

"Soyez cyber-chouette" fait référence à l'animal "une chouette" qui a beaucoup d'intuition, d'intelligence et de sagesse. L'expression "être chouette" signifie le fait d'être joli, élégant et digne d'admiration.

Soyez cyber-chouette !

Prochaine leçon :
L'internet des objets (Ido)

Diapositive 20 ;

La leçon # 8 portera sur les objets connectés aussi appelés ; l'internet des objets (Ido).



Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
Créatifs



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



Diapositive 21 ;

Labos créatifs est un organisme sans but lucratif qui aide les écoles à développer une culture de la créativité et d'innovation. Leur site web est ;
<https://www.laboscreatifs.ca/>



Sites Web utiles pour la leçon # 7

Avertissement : Nous utilisons des hyperliens provenant de différentes sources sur internet. Certaines publicités s'y retrouvent sûrement. Avant d'utiliser un hyperlien en classe, il est essentiel de prendre un moment pour le vérifier en privé afin de vous assurer que celui-ci est utilisable en classe avec vos élèves. Nous l'avons vérifié avant de vous le suggérer, mais il est possible qu'avec le temps, le contenu ait été redirigé, modifié ou éliminé. Il est même possible que certaines publicités aient été modifiées et que celles-ci vous rendent inconfortable. Au final, c'est à vous de décider si vous voulez utiliser ou non un hyperlien en salle de classe avec vos élèves. Nous préférons vous en avertir.

- | **Labo créatif** | Lien officiel de l'organisme | Site Web ; <https://www.laboscreatifs.ca/>
- | **Labo créatif** | **Liens francophones pour éduquer à la cybersécurité** | Site Web ;
<https://www.laboscreatifs.ca/cybersecurite-ressources>
- | **HabiloMédias** | **La section Cybersécurité d'HabiloMédias** | Site Web ;
<https://habilomedias.ca/litteratie-numerique-et-education-aux-medias/enjeux-numeriques/cybersécurité>
- | **TerraNova Security (entreprise privée)** | **Qu'est-ce que le piratage psychologique?** | Document PDF ;
<https://terrannovasecurity.com/wp-content/uploads/2021/09/What-Is-Social-Engineering-FR-CA.pdf>
- | **Conscio Technologies (entreprise privée)** | **Une introduction à l'ingénierie sociale** | Vidéo YouTube ;
https://youtu.be/LER3_tp9vp4
- | **Conscio Technologies (entreprise privée)** | **Ingénierie sociale, les bons réflexes** | Vidéo YouTube ;
<https://youtu.be/fuNqsFXqQOU>
- | **Conscio Technologies (entreprise privée)** | **Ingénierie sociale, anatomie d'une attaque classique** | Vidéo YouTube ;
https://youtu.be/lbetgF2f_58
- | **RTI Officiel** | **2 minutes pour comprendre la cybersécurité** | Vidéo YouTube ;
<https://youtu.be/S1kNXCdMgVI>



Leçon # 7

Apprendre à se protéger
pour les élèves du primaire

L'ingénierie sociale est un
autre type de piège de la
cybersécurité.

LABOS
LABOS
LABOS



Leçon # 7 : L'ingénierie sociale est un autre type de piège de la cybersécurité.



Suggestions d'activités complémentaires

Ces activités peuvent être modifiées et adaptées selon l'âge de vos élèves. L'important ici, c'est d'essayer de faire des transferts avec la leçon.

- Préparer des affiches avec des conseils sur l'ingénierie sociale.
- Tenir à jour une liste de mots importants ou créer votre propre glossaire de la cybersécurité.
- Faire une entrevue avec un expert de l'informatique et l'ingénierie sociale.
- Trouver des statistiques à propos de l'ingénierie sociale sur des sites reconnus.
- Inventer une histoire avec une aventure en cybersécurité
- Faire une courte présentation à une autre classe de ce que vous avez appris au sujet de l'importance d'apprendre à se protéger et de mieux connaître ce qu'est l'ingénierie sociale.
- Inventer un jeu questionnaire de la cybersécurité.
- Créer une courte vidéo pour enseigner comment mieux se protéger en ligne.
- Aller visiter une classe de votre école et expliquez ce que vous avez appris avec cette leçon.
- Proposer à la direction de votre école, la création d'une brigade de la cybersécurité afin d'aider les autres élèves et de leur apprendre à mieux se protéger au niveau de la cybersécurité.
- Créer une campagne de sensibilisation en préparant des affiches et placez celles-ci un peu partout dans votre école.
- Inventer un super-héros de la cybersécurité pour votre classe et inventez des histoires que vous pourrez écrire sous forme de livrets avec vos propres dessins.
- Faire une recherche sur les chouettes et trouver pourquoi ces oiseaux ont beaucoup d'intuition, d'intelligence et de sagesse.
- Faire une étude sur les renards et trouver pourquoi ces animaux sont très rusés et comment ils réussissent à déjouer les pièges et les agriculteurs de poulets.
- Faire un tableau avec une liste d'exemples des pièges possibles de l'ingénierie sociale
- Dénichez des articles de presse au sujet de l'ingénierie sociale et présentez un article que vous avez aimé avec les membres votre famille.



Leçon # 8

Apprendre à se protéger
pour les élèves du primaire

L'internet des objets
(Ido), il est important de
connaître les risques.

LABOS



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



Objectif de cette leçon

Avec la leçon # 8, les élèves pourront comprendre ce que c'est l'Internet des objets (IdO) et des moyens pour apprendre à mieux se protéger.

Démarche proposée

Nous vous suggérons tout simplement de prendre un moment dans la journée pour passer en revue les différentes diapositives de la leçon # 8 et d'avoir une discussion avec vos élèves concernant les pièges de la cybersécurité. Il n'est pas nécessaire d'avoir de grandes connaissances dans le domaine. Grâce aux diapositives de la leçon # 8 du programme "**Soyez cyber-chouette !**" comme support pédagogique, vous pourrez facilement présenter de nouveaux concepts et des mots importants ainsi que le jargon du monde de la cybersécurité. L'important ici sera de prendre un temps d'arrêt et d'avoir cette discussion unique et essentielle avec vos élèves.

Questions d'objectivation

Voici quelques exemples de questions d'objectivations qui pourraient être utiles pendant ou après avoir visionné la leçon. N'hésitez pas à les modifier ou à y ajouter vos propres questions au besoin ;

- **Élèves de la maternelle à la 3^e année ;**
 - Utilisez-vous des objets connectés à la maison ?
 - Comment est-ce que des objets connectés peuvent être utiles ?
 - Est-ce qu'il y a des risques à utiliser des objets connectés ?
- **Élèves de 4^e à la 6^e année ;**
 - Comment est-ce que des objets connectés peuvent être utiles ? Avez-vous des exemples ?
 - Est-ce qu'il y a des risques à utiliser des objets connectés ?
 - Quels seraient des avantages et des inconvénients d'utiliser des objets connectés ?
 - Quels seraient des conseils à donner à des personnes qui veulent utiliser des objets connectés ?
 - Avez-vous appris quelque chose de nouveau aujourd'hui ? Expliquez ?



Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

LABOS créatifs



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



Soyez cyber-chouette!

Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

LABOS créatifs



Diapositive 1 ;

L'objectif de la leçon # 8 est de comprendre ce que c'est l'ingénierie sociale et de réaliser l'importance de ne pas paniquer lorsqu'on doit prendre une décision importante.

Diapositive 2 ;

L'internet des objets (souvent aussi désigné par Ido) est lorsque des objets doivent être connectés à Internet pour fonctionner ou pour offrir une plus grande expérience d'utilisation.

Diapositive 3 ;

L'Ido est souvent proposé pour nous faciliter la vie ou pour rendre notre maison beaucoup plus sécuritaire.

Diapositive 4 ;

Les élèves ont probablement plusieurs d'idées d'objets utilisés dans leur foyer qui utilise l'Internet des objets. On pourra penser au contrôle des lumières et de la température. Les systèmes de sécurité et de contrôle à distance.

 **L'internet des objets, qu'est-ce que c'est ?**

L'Internet des objets, c'est quand des choses à la maison, comme des jouets et des gadgets, utilisent Internet pour faire des choses spéciales.



Connaissez-vous des exemples d'objets utilisés à la maison et qui utilisent l'internet pour fonctionner ?



Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

LABOS



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



Des exemples d'objets connectés pourraient être des :

montres



appareils ménagers



appareils lumineux



systèmes de sécurité



thermomètres



voitures intelligentes



Diapositive 5 ;

Nous avons déjà à la maison plusieurs appareils qui utilisent l'Internet des objets. Il y a de plus en plus d'objets connectés à travers la planète. Ce nombre augmente sans cesse.

Diapositive 6 ;

Il est important de bien connaître les dangers de l'utilisation des objets connectés à l'internet, car ceux-ci deviennent des portes d'entrées pour les pirates informatiques si ces objets sont peu sécurisés.

Diapositive 7 ;

Les personnes aiment souvent que la vie soit plus facile et les entreprises l'ont bien compris. Celles-ci nous offrent de plus en plus d'appareils que nous pouvons brancher à Internet. Mais, est-ce bien nécessaire ?

Diapositive 8 ;

Les objets connectés à Internet sont variés et on prévoit qu'avec le développement de la robotique et des voitures intelligentes, l'Ido sera de plus en plus présent dans nos vies. Nous devons nous adapter et apprendre à se protéger.

Comment est-ce que ça fonctionne ?



Nous aimons avoir la vie facile et les objets connectés peuvent nous aider à faire plusieurs tâches autour de la maison.



Par exemple, des objets connectés existent pour ouvrir les lumières automatiquement ou pour changer la température à l'intérieur de la maison sans se lever.





Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

LABOS



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



Le problème est que ces objets connectés deviennent des portes d'entrées pour les cyberpirates qui pourront ainsi accéder à d'autres appareils sur notre réseau.



Diapositive 9 ;

Les objets connectés qui ne sont pas sécurisés par un mot de passe fort, par exemple, peuvent permettre à des cyberpirates de les bloquer ou d'accéder à d'autres appareils que nous avons à la maison.

Et, il y en a de plus en plus d'objets connectés partout sur la planète !



Diapositive 10 ;

Selon certaines sources, il y aurait présentement plus de 17 milliards d'appareils Ido dans le monde. Ce nombre devrait atteindre près de 30 milliards d'ici à 2030.



Il est donc très important que ces objets connectés soient fiables, sécuritaires et bien protégés par des mots de passe forts.

Diapositive 11 ;

Avant de brancher un nouvel objet connecté à Internet, on devrait s'assurer qu'il est fiable, sécuritaire et que le mot de passe du fabricant (qui est généralement très facile) soit remplacé par un mot de passe fort.

Il faut aussi, à l'occasion, se demander s'ils sont vraiment nécessaires et si ce serait plus sécuritaire de s'en passer.



Diapositive 12 ;

On peut se demander si cela est vraiment nécessaire à acheter ou à installer dans notre maison. Certains appareils de l'Ido peuvent envoyer vos informations personnelles à une partie tierce ou même avoir un micro qui est automatiquement activé dans l'appareil.



Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

LABOS



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



C'est pour cela qu'il est super important d'apprendre à bien se protéger !

Diapositive 13 ;

Ce qui est important ici, c'est de s'assurer que les élèves comprennent que ces objets connectés viennent avec des avantages et des désavantages. Il faut juste s'en rappeler.

Des trucs utiles...

- Certains objets connectés recueillent des renseignements personnels et peuvent les offrir à d'autres personnes. Lisez attentivement les informations à propos de vos objets connectés.
- Vérifiez si vous pouvez utiliser votre objet connecté sans que vos informations soient partagées.
- Réglez votre appareil pour que le Wi-Fi et le Bluetooth soient désactivés lorsque vous ne les utilisez pas.

Source: Commissariat à la protection de la vie privée du Canada

Diapositive 14 ;

Ces trucs seront probablement difficiles à retenir pour les élèves. L'important, c'est de comprendre qu'il y a des choses qu'on peut faire pour se protéger et qu'on devrait toujours demander de l'aide à un adulte de confiance.

Des trucs utiles...

- Changez le mot de passe par défaut de l'appareil (s'il y en a un) puisque les mots de passe par défaut sont souvent faciles à deviner et bien connus des pirates informatiques.
- Au moment de l'inscription, ne fournissez que les renseignements nécessaires : utilisez un pseudonyme au lieu de votre nom et ne donnez jamais votre véritable date de naissance.

Source: Commissariat à la protection de la vie privée du Canada

Diapositive 15 ;

L'utilisation d'un mot de passe fort est important lorsqu'on essaie de brancher des objets connectés sur Internet. C'est une belle occasion pour réviser avec les élèves ce qu'est un mot de passe fort.

Des trucs utiles...

- Il faut s'assurer de faire les mises à jour de vos logiciels et de vos appareils régulièrement.
- Il faut s'assurer d'avoir une copie de sauvegarde de ses fichiers séparément de votre réseau si possible.
- Il faut toujours demander de l'aide à un adulte de confiance si vous désirez installer de nouveaux objets connectés sur le réseau à la maison ou ailleurs.

Source: Commissariat à la protection de la vie privée du Canada

Diapositive 16 ;

Il est très important de toujours faire la mise à jour lorsqu'on utilise un objet connecté à Internet. C'est aussi le cas pour tous les ordinateurs et appareils cellulaires à la maison. C'est une façon simple et efficace de se protéger.



Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

LABOS



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



Enfin...

Généralement, les objets connectés que nous utilisons à la maison sont installés par les adultes qui vivent chez-nous.

Il est important de se rappeler que ces objets connectés peuvent recueillir des données personnelles et sensibles.

Il faut donc être très vigilant !



Diapositive 17 ;

Voici une belle occasion de revoir ce que sont les données personnelles et sensibles et de rappeler aux élèves de toujours vérifier avec un adulte de confiance s'ils ont des questions.

Leçon # 8

L'internet des objets (Ido), il est important de connaître les risques !



Diapositive 18 ;

C'est la leçon à retenir. L'internet des objets (Ido) peut présenter des risques graves si on ne fait pas attention.

Soyez cyber-chouette!



Diapositive 19 ;

"Soyez cyber-chouette" fait référence à l'animal "une chouette" qui a beaucoup d'intuition, d'intelligence et de sagesse. L'expression "être chouette" signifie le fait d'être joli élégant et digne d'admiration.

Soyez cyber-chouette !

Prochaine leçon :
L'intelligence artificielle (IA)

Diapositive 20 ;

La leçon # 9 portera sur l'intelligence artificielle (IA).



Leçon # 8

Apprendre à se protéger pour les élèves du primaire

L'internet des objets (Ido), il est important de connaître les risques.

LABOS Créatifs



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



Diapositive 21 ;

Labos créatifs est un organisme sans but lucratif qui aide les écoles à développer une culture de la créativité et d'innovation. Leur site web est ; <https://www.laboscreatifs.ca/>

Sites Web utiles pour la leçon # 8

Avertissement : Nous utilisons des hyperliens provenant de différentes sources sur internet. Certaines publicités s'y retrouvent sûrement. Avant d'utiliser un hyperlien en classe, il est essentiel de prendre un moment pour le vérifier en privé afin de vous assurer que celui-ci est utilisable en classe avec vos élèves. Nous l'avons vérifié avant de vous le suggérer, mais il est possible qu'avec le temps, le contenu ait été redirigé, modifié ou éliminé. Il est même possible que certaines publicités aient été modifiées et que celles-ci vous rendent inconfortable. Au final, c'est à vous de décider si vous voulez utiliser ou non un hyperlien en salle de classe avec vos élèves. Nous préférons vous en avertir.

- **Labo créatif** | Lien officiel de l'organisme | Site Web ; <https://www.laboscreatifs.ca/>
- **Labo créatif** | **Liens francophones pour éduquer à la cybersécurité** | Site Web ; <https://www.laboscreatifs.ca/cybersecurite-ressources>
- **HabiloMédias** | **La section Cybersécurité d'HabiloMédias** | Site Web ; <https://habilomedias.ca/litteratie-numerique-et-education-aux-medias/enjeux-numeriques/cybersécurité>
- **RTI Officiel** | **2 minutes pour comprendre la cybersécurité** | Vidéo YouTube ; <https://youtu.be/S1kNXCdMgVI>
- **Waya Tech** (entreprise privée) | **3 minutes pour comprendre... Les objets connectés** | Vidéo YouTube ; <https://youtu.be/qPh8N01447E>
- **Investigation et Enquêtes** | **Comment un hacker peut espionner toute notre maison** | Vidéo YouTube ; <https://youtu.be/Q13WvaQetcQ>
- **France24** | **Comment un Viking avec une dent bleue a donné son nom au Bluetooth** | Article de presse ; <https://www.france24.com/fr/20170124-comment-viking-une-dent-bleue-a-donne-son-nom-bluetooth>



Leçon # 8

Apprendre à se protéger
pour les élèves du primaire

L'internet des objets
(Ido), il est important de
connaître les risques.

LABOS



Leçon 8 : L'internet des objets (Ido), il est important de connaître les risques.



Suggestions d'activités complémentaires

Ces activités peuvent être modifiées et adaptées selon l'âge de vos élèves. L'important ici, c'est d'essayer de faire des transferts avec la leçon.

- Réaliser un petit sondage sur l'utilisation des objets connectés à la maison.
- Préparer des affiches avec des conseils sur l'utilisation d'objets connectés.
- Tenir à jour une liste de mots importants ou créer votre propre glossaire de la cybersécurité.
- Faire une entrevue avec un expert de l'informatique et l'utilisation d'objets connectés.
- Trouver des statistiques à propos de l'Ido sur des sites reconnus.
- Inventer une histoire avec une aventure en cybersécurité
- Faire une courte présentation à une autre classe de ce que vous avez appris au sujet de l'importance d'apprendre à se protéger lorsqu'on utilise l'Internet des objets (Ido).
- Inventer un jeu questionnaire de la cybersécurité.
- Créer une courte vidéo pour enseigner comment mieux se protéger en ligne.
- Aller visiter une classe de votre école et expliquez ce que vous avez appris avec cette leçon.
- Proposer à la direction de votre école, la création d'une brigade de la cybersécurité afin d'aider d'autres élèves et de leur apprendre à mieux se protéger au niveau de la cybersécurité.
- Créer une campagne de sensibilisation en préparant des affiches et placez celles-ci un peu partout dans votre école.
- Inventer un super-héros de la cybersécurité pour votre classe et inventez des histoires que vous pourrez écrire sous forme de livrets avec vos propres dessins.
- Faire une recherche sur les chouettes et trouver pourquoi ces oiseaux ont beaucoup d'intuition, d'intelligence et de sagesse.
- Faire une liste possible de tous les appareils pouvant utiliser l'internet des objets (Ido).
- Faire un inventaire des objets connectés dans votre foyer ou dans votre école.
- Faire un tableau en deux colonnes avec une liste des avantages d'utiliser des objets connectés d'un côté et les désavantages de l'autre.
- Inviter une personne à faire une démonstration de l'utilisation d'un objet connecté.



Leçon # 9

Apprendre à se protéger
pour les élèves du primaire

l'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.

LABOS
LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



Objectif de cette leçon

Dans la leçon # 9, les élèves comprendront ce qu'est l'intelligence artificielle (IA) et pourront nommer des façons de se protéger en l'utilisant tout en faisant attention aux "hallucinations de l'IA."

Démarche proposée

Nous vous suggérons tout simplement de prendre un moment dans la journée pour passer en revue les différentes diapositives de la leçon # 9 et d'avoir une discussion avec vos élèves concernant les pièges de la cybersécurité. Il n'est pas nécessaire d'avoir de grandes connaissances dans le domaine. Grâce aux diapositives de la leçon # 9 du programme "**Soyez cyber-chouette !**" comme support pédagogique, vous pourrez facilement présenter de nouveaux concepts et des mots importants ainsi que le jargon du monde de la cybersécurité. L'important ici sera de prendre un temps d'arrêt et d'avoir cette discussion unique et essentielle avec vos élèves.

Questions d'objectivation

Voici quelques exemples de questions d'objectivations qui pourraient être utiles pendant ou après avoir visionné la leçon. N'hésitez pas à les modifier ou à y ajouter vos propres questions au besoin ;

- **Élèves de la maternelle à la 3^e année ;**
 - C'est quoi être intelligent selon vous ?
 - Est-ce que les ordinateurs sont intelligents ? Pourquoi ?
 - Est-ce que les ordinateurs peuvent nous aider à faire de bonnes choses ?
 - Après cette leçon, que pensez-vous de l'Intelligence artificielle (IA) ? Est-ce important ?
- **Élèves de 4^e à la 6^e année ;**
 - Avez-vous déjà entendu parler de l'intelligence artificielle (IA) ? C'est quoi selon vous ? Est-ce essentiel ?
 - Qu'est-ce que vous aimeriez savoir au sujet de l'IA ?
 - Que savez-vous maintenant au sujet de l'IA que vous ne connaissez pas avant cette leçon ?
 - Connaissez-vous de l'utilisation de l'utilisation positive de l'IA pour aider les personnes ?
 - Où sera l'IA dans 5 ans, dans 10 ans, dans 50 ans ou même dans 100 ans ?



Leçon # 9

Apprendre à se protéger pour les élèves du primaire

l'intelligence artificielle (IA), il faut faire attention aux hallucinations.

LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



Soyez cyber-chouette!

Leçon # 9

Apprendre à se protéger pour les élèves du primaire

l'intelligence artificielle (IA), il faut faire attention aux hallucinations.

LABOS



Diapositive 1 ;

L'objectif de la leçon # 9 est de comprendre ce qu'est l'intelligence artificielle (IA) et pourront nommer des façons de se protéger en l'utilisant tout en faisant attention aux "hallucinations de l'IA."

L'intelligence artificielle, qu'est-ce que c'est ?



Diapositive 2 ;

Prendre un moment pour avoir une discussion et pour faire une liste de réponses possibles. On peut même en faire une liste au tableau.

L'intelligence artificielle (IA), c'est quand un ordinateur peut apprendre à faire des choses intelligentes comme nous.



Source ; ChatGPT

Diapositive 3 ;

L'intelligence artificielle, souvent désignée par "IA", est cette capacité qu'ont les ordinateurs de pouvoir apprendre et à faire certaines choses dans le but de nous aider. On s'attend que cette facilité continue de s'améliorer avec le temps.

Par exemple, lorsqu'un ordinateur peut reconnaître des images, donner des conseils en ligne ou même conduire des voitures !



Source ; ChatGPT

Diapositive 4 ;

Des exemples de l'intelligence artificielle sont ; la reconnaissance d'images par des caméras branchées, des sites interactifs pour des conseils en ligne ou même la conduite indépendante de voitures.



Leçon # 9

Apprendre à se protéger
pour les élèves du primaire

l'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.

LABOS
LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.




**Comment
est-ce que ça
fonctionne ?**

Diapositive 5 ;

Prendre un moment pour poser la question aux élèves et de voir quelles sont leurs hypothèses.

L'intelligence artificielle, c'est comme si on apprenait aux ordinateurs à réfléchir et à résoudre des problèmes tout seuls, pour qu'ils deviennent des super-héros électroniques !



Source : ChatGPT

Diapositive 6 ;

L'IA est la possibilité qu'ont les ordinateurs à emmagasiner une quantité incroyable de données et d'en faire l'analyse, la classification et de réussir à faire des liens entre celles-ci pour pouvoir mieux les partager à nouveau.

Les ordinateurs peuvent s'entraîner à réfléchir grâce à ce qu'on appelle des "algorithmes d'apprentissage".




Source : ChatGPT

Diapositive 7 ;

Les algorithmes sont des programmes informatiques qui contiennent une série d'étapes à suivre pour résoudre un problème ou faire quelque chose de spécial avec l'aide d'un ordinateur.

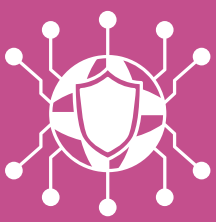
C'est un peu comme donner à un ordinateur des jeux ou des exercices à faire pour qu'il devienne de plus en plus fort et intelligent avec le temps.



Source : ChatGPT

Diapositive 8 ;

Pour développer de bons algorithmes en intelligence artificielle, on doit analyser les données, et les modèles mathématiques pour ensuite tester plusieurs fois ceux-ci pour s'assurer qu'ils prennent de bonnes décisions.



Leçon # 9

Apprendre à se protéger
pour les élèves du primaire

l'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.

LABOS
LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



L'IA peut être bonne
quand elle nous aide à
résoudre des problèmes.
En revanche, soyons
gentil avec elle en lui
apprenant de bonnes
choses pour qu'elle fasse
du bien aux personnes.

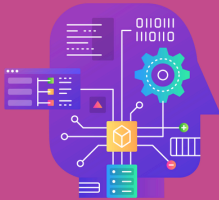


Source : ChatGPT

Diapositive 9 ;

L'IA est efficace lorsque les humains construisent de bons algorithmes et lorsque les ordinateurs s'entraînent à faire de bons liens avec les informations qu'on lui transmet. L'IA va continuer d'évoluer au courant des prochaines années.

L'IA peut présenter
certains dangers. Par
exemple, elle peut
faire des erreurs
importantes ou ne pas
respecter la vie privée
des personnes.



Source : ChatGPT

Diapositive 10 ;

L'IA peut se tromper et faire des erreurs. Il est aussi dangereux que certaines informations personnelles et sensibles se retrouve dans ses données. Nous devons demeurer vigilants en tout temps.

C'est ce que l'on
appelle des
hallucinations d'IA
qui sont des fausses
informations dans
des sujets importants



Diapositive 11 ;

L'expression "hallucinations de l'IA" est de plus en plus utilisée pour nommer les déformations et les erreurs générées par l'IA dans des sujets importants comme en santé ou en histoire.

Pour se protéger de l'IA, soyons conscient de ce qu'on partage en ligne, ne pas donner des informations personnelles et sensibles à des sites ou des personnes qu'on ne connaît pas, et en parler avec un adulte de confiance si on a des doutes.

Source : ChatGPT

Diapositive 12 ;

Comme nous l'avons vu précédemment dans les autres leçons, il est important de continuer à ne pas partager nos informations personnelles et toujours en parler avec un adulte de confiance si nous ne sommes pas certains de ce qui se passe.



Leçon # 9

Apprendre à se protéger pour les élèves du primaire

l'intelligence artificielle (IA), il faut faire attention aux hallucinations.

LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



Avec l'IA, on entend souvent parler ChatGPT, mais cela pourrait aussi être des robots qui aident à nettoyer la maison, des jeux vidéo intelligents qui s'adaptent à nous, ou bien des traducteurs qui comprennent et parlent différentes langues !

Source : ChatGPT

Diapositive 13 ;

L'IA continue d'évoluer et sera de plus en plus présente dans notre vie au quotidien. De plus en plus d'entreprises offrent des services d'IA sur internet. Il est important de faire attention avec les outils qu'on utilise.

L'avenir de l'IA ?

L'avenir de l'IA est excitant, car elle pourrait nous aider à résoudre de grands défis et rendre la vie meilleure pour tout le monde.



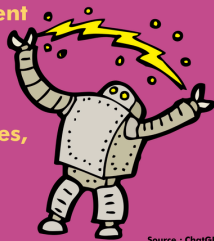
Source : ChatGPT

Diapositive 14 ;

L'avenir de l'IA est difficile à prédire, mais assurément, elle évoluera et ces changements seront de plus en plus rapides. Il y a du positif à cela et il peut aussi y avoir des effets négatifs.

L'avenir de l'IA...

Certaines personnes craignent que l'IA devient trop puissante ou qu'elle prenne des décisions sans toujours comprendre les conséquences, comme dans les films de science-fiction.



Source : ChatGPT

Diapositive 15 ;

Certaines personnes sont très négatives à l'idée que l'IA prend une place de plus en plus grande dans le monde. Ce qui est certain, c'est que le développement de l'IA est commencé et qu'il semble être impossible à arrêter.

C'est pour cela qu'il est super important d'apprendre au sujet de l'IA et de savoir comment bien se protéger !



Diapositive 16 ;

Notre plus grande défense concernant l'IA est de demeurer vigilant en tout temps et de ne pas partager nos informations personnelles et sensibles. Il faut aussi choisir nos outils de l'IA avec soin et avec un bon jugement.



Leçon # 9

Apprendre à se protéger
pour les élèves du primaire

l'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.

LABOS
LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



L'as-tu remarqué ?

Les sources d'information de
cette présentation ont presque
été entièrement réalisées par
l'IA !

Source : ChatGPT

Diapositive 17 ;

Cette présentation a été préparée par un humain qui a utilisé ChatGPT pour trouver la plupart des informations utilisées sur les diapositives de la leçon 9. Cet humain a aussi validé les informations grâce à d'autres sources avant de les utiliser.

Leçon # 9

l'intelligence
artificielle (IA), il
faut faire attention
aux hallucinations.



Diapositive 18 ;

C'est la leçon à retenir. Nous devons demeurer vigilants en tout temps avec l'intelligence artificielle (IA) et faire attention aux hallucinations d'IA.

Soyez cyber-chouette!



Diapositive 19 ;

"Soyez cyber-chouette" fait référence à l'animal "une chouette" qui a beaucoup d'intuition, d'intelligence et de sagesse. L'expression "être chouette" signifie le fait d'être joli élégant et digne d'admiration.

Soyez cyber-chouette !

Prochaine leçon :
Les villes intelligentes et
la cybersécurité

Diapositive 20 ;

La leçon # 10 portera sur les villes intelligentes et la cybersécurité.



Leçon # 9

Apprendre à se protéger
pour les élèves du primaire

l'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.

LABOS
Créatifs



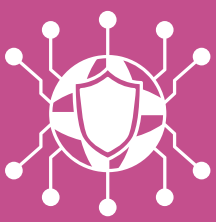
Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



Diapositive 21 ;

Labos créatifs est un organisme sans but lucratif qui aide les écoles à développer une culture de la créativité et d'innovation. Leur site web est ;

<https://www.laboscreatifs.ca/>



Leçon # 9

Apprendre à se protéger
pour les élèves du primaire

l'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.

LABOS
LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



Sites Web utiles pour la leçon # 9

Avertissement : Nous utilisons des hyperliens provenant de différentes sources sur internet. Certaines publicités s'y retrouvent sûrement. Avant d'utiliser un hyperlien en classe, il est essentiel de prendre un moment pour le vérifier en privé afin de vous assurer que celui-ci est utilisable en classe avec vos élèves. Nous l'avons vérifié avant de vous le suggérer, mais il est possible qu'avec le temps, le contenu ait été redirigé, modifié ou éliminé. Il est même possible que certaines publicités aient été modifiées et que celles-ci vous rendent inconfortable. Au final, c'est à vous de décider si vous voulez utiliser ou non un hyperlien en salle de classe avec vos élèves. Nous préférons vous en avertir.

- | **Labo créatif** | Lien officiel de l'organisme | Site Web ; <https://www.laboscreatifs.ca/>
- | **Labo créatif** | **Liens francophones pour éduquer à la cybersécurité** | Site Web ; <https://www.laboscreatifs.ca/cybersecurite-ressources>
- | **HabiloMédias** | **La section Cybersécurité d'HabiloMédias** | Site Web ; <https://habilomedias.ca/litteratie-numerique-et-education-aux-medias/enjeux-numeriques/cybersécurité>
- | **Curionauts des sciences** | **C'est quoi l'intelligence artificielle ?** | Vidéo YouTube ; https://www.youtube.com/watch?v=PBJ9_G8d6mo
- | **TiDoc'** | **Qu'est-ce que c'est l'intelligence artificielle ?** | Vidéo YouTube ; <https://www.youtube.com/watch?v=XUac2v2oVBA>
- | **TiDoc'** | **Comment fonctionne l'intelligence artificielle ?** | Vidéo YouTube ; <https://www.youtube.com/watch?v=bpbt2jlpwPs>
- | **TiDoc'** | **Qui sont les meilleurs amis de l'intelligence artificielle ?** | Vidéo YouTube ; <https://www.youtube.com/watch?v=5DK4LHkpp4E>
- **Digital Moment** (anciennement Kids Code Jeunesse) | **Mais qu'est-ce qu'un algorithme ?** | Vidéo YouTube ; <https://www.youtube.com/watch?v=2oegxbYUFAs>
- | **Bayard** | Le magazine Astrapi explique les secrets de l'IA aux 7-11 ans | **C'est quoi l'intelligence artificielle ?** | Article en format PDF ; <https://www.astrapi.com/wp-content/uploads/sites/31/2023/09/Astrapi-1022-octobre-2023-intelligence-artificielle.pdf>
- | **Bayard** | **Un quiz pour apprendre à repérer les images créées à l'aide d'une intelligence artificielle** | Jeu interactif en ligne ; https://www.astrapi.com/wp-content/uploads/sites/31/quiz-ia/#utm_medium=ref&utm_source=bayard-jeunesse.com&utm_campaign=autopromo&utm_content=quiz



Leçon # 9

Apprendre à se protéger
pour les élèves du primaire

l'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.

LABS LABOS



Leçon # 9 : L'intelligence artificielle (IA), il faut faire attention aux hallucinations.



Suggestions d'activités complémentaires

Ces activités peuvent être modifiées et adaptées selon l'âge de vos élèves. L'important ici, c'est d'essayer de faire des transferts avec la leçon.

- Réaliser un petit sondage sur la cybersécurité en général et pour mesurer si les personnes en savent ce qu'est l'Intelligence artificielle (IA) ou non. On peut aussi mesurer leurs perceptions.
- Préparer des affiches avec des informations pour présenter l'IA, les points positifs et les dangers.
- Tenir à jour une liste de mots importants ou créer votre propre glossaire de la cybersécurité.
- Faire une entrevue avec un expert de l'informatique au sujet de l'IA.
- Trouver des statistiques sur le développement de l'IA à partir de sites reconnus.
- Créer une histoire avec une aventure en cybersécurité.
- Faire une courte présentation à une autre classe de ce que vous avez appris au sujet de l'IA.
- Inventer un jeu questionnaire de la cybersécurité et sur l'IA.
- Créer une courte vidéo pour enseigner ce qu'est l'IA et expliquer pourquoi c'est de plus en plus important.
- Proposer à la direction de votre école, la création d'une brigade de la cybersécurité afin d'aider d'autres élèves et de leur apprendre à mieux se protéger au niveau de la cybersécurité.
- Créer une campagne de sensibilisation en préparant des affiches et placez celles-ci un peu partout dans votre école.
- Inventer un super-héros de la cybersécurité pour votre classe et inventez des histoires que vous pourrez écrire sous forme de livrets avec vos propres dessins.
- Créer une petite pièce et la jouer avec un théâtre de marionnettes.
- Utilisez "cyber-chouette" pour créer et résoudre des problèmes de mathématiques ou pour écrire des histoires de détectives qui partent en mission.
- Écrire une lettre à ses parents ou à des membres de sa famille qui explique les meilleures façons de se protéger en cybersécurité et qui présente ce qu'est l'IA.
- Organiser un concours avec des slogans de protection en cybersécurité.



Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABS LABOS



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Objectif de cette leçon

Dans la leçon # 10, les élèves comprendront ce que sont les villes intelligentes et de mieux comprendre les avantages et les dangers de celles-ci.

Démarche proposée

Nous vous suggérons tout simplement de prendre un moment dans la journée pour passer en revue les différentes diapositives de la leçon # 10 et d'avoir une discussion avec vos élèves concernant les pièges de la cybersécurité. Il n'est pas nécessaire d'avoir de grandes connaissances dans le domaine. Grâce aux diapositives de la leçon # 10 du programme "**Soyez cyber-chouette!**" comme support pédagogique, vous pourrez facilement présenter de nouveaux concepts et des mots importants ainsi que le jargon du monde de la cybersécurité. L'important ici sera de prendre un temps d'arrêt et d'avoir cette discussion unique et essentielle avec vos élèves.

Questions d'objectivation

Voici quelques exemples de questions d'objectivations qui pourraient être utiles pendant ou après avoir visionné la leçon. N'hésitez pas à les modifier ou à y ajouter vos propres questions au besoin ;

- **Élèves de la maternelle à la 3^e année ;**
 - C'est quoi selon vous une ville intelligente ? Avez-vous des exemples ?
 - Quels sont les avantages d'une ville intelligente ?
- **Élèves de 4^e à la 6^e année ;**
 - C'est quoi selon vous une ville intelligente ? Avez-vous des exemples ?
 - Quelles sont les qualités d'une ville intelligente ?
 - Est-ce qu'il y aurait des désavantages ?
 - Est-ce que la cybersécurité est importante pour les villes intelligentes ? Pourquoi ?
 - Comment est-ce que les villes intelligentes peuvent se protéger ?
 - À quoi pourrait ressembler des villes intelligentes du futur ?
 - Quelles pourraient être des différences entre des villes anciennes et des villes du futur ?



Soyez cyber-chouette!

Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABOS
LABOS



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Soyez cyber-chouette!

Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABOS
LABOS



Diapositive 1 ;

L'objectif de la leçon # 10 est de mieux comprendre ce que sont les villes intelligentes (*aussi souvent appelé Smart City en France*) et de mieux comprendre les avantages et les dangers de celles-ci.

Diapositive 2 ;

Demander aux élèves de dire ce qu'ils savent au sujet des villes intelligentes.



Une ville intelligente, qu'est-ce que c'est ?

Une ville intelligente, c'est une communauté où les maisons, les routes et les parcs peuvent échanger entre eux pour rendre la vie des personnes plus facile et plus sécuritaire.



Diapositive 3 ;

Les villes intelligentes ont des systèmes informatiques qui peuvent communiquer entre eux. Par exemple, pour connaître la température d'un bâtiment sans avoir à y aller grâce à un site internet et un capteur installé à l'intérieur de celui-ci.

Les villes intelligentes sont très importantes, car elles aident à rendre nos maisons plus sûrs, nos déplacements plus faciles et aident la Terre grâce à moins d'énergie et à moins de déchets.



Source : ChatGPT

Diapositive 4 ;

Dans les villes intelligentes, plusieurs systèmes communiquent entre eux (par seulement la température) pour agir et pour que la ville soit plus sécuritaire, efficace et meilleure pour l'environnement.

Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABS LABOS



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Comment
est-ce que ça
fonctionne ?

Diapositive 5 ;

Vous pouvez en profiter pour faire un petit rappel à propos de la leçon # 8 sur les objets connectés et l'Internet des objets (Ido).

En général, les objets connectés utilisent des données, des sondes de températures ou des caméras pour démarrer ou arrêter certains appareils dans les maisons et les édifices.



Diapositive 6 ;

Dans une ville intelligente, il y a beaucoup d'objets connectés et qui utilisent l'Internet des objets (Ido) pour fonctionner entre eux. Ça peut facilement devenir complexe.



Dans les villes intelligentes, les ordinateurs aident à rendre les maisons plus confortables, les rues plus sûres et à trouver facilement ce dont on a besoin !

Source : ChatGPT

Diapositive 7 ;

Il y a des avantages comme le fait de rendre nos maisons plus confortables, les rues sécuritaires et nous permettre de trouver des informations importantes lorsque nous en avons de besoin.

Dans les villes intelligentes, la cybersécurité ressemble à un bouclier magique qui garde les ordinateurs et les informations en sécurité, afin que tout fonctionne parfaitement !



Source : ChatGPT

Diapositive 8 ;

Dans les villes intelligentes, la cybersécurité est très importante pour s'assurer que tout fonctionne en tout temps. Cependant, les villes peuvent être victimes des cyberpirates qui utilisent souvent des rançongiciels pour paralyser le fonctionnement de certains services.

Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABS LABOS



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Un exemple ;

Les feux de circulation qui s'adaptent à la circulation des voitures en temps réel, permettant ainsi aux voitures de rouler plus facilement.



Diapositive 9 ;

Les feux de circulation qui s'adaptent en temps réel sont un bel exemple d'une utilisation d'objets connectés par une ville intelligente. Il y a ainsi moins de voitures qui attendent pour rien, ce qui réduit les émissions de gaz carbonique (CO₂).

Un autre exemple ;

Les poubelles connectées qui signalent quand elles sont pleines, permettant aux services de collecte de les ramasser plus rapidement.



Source : ChatGPT

Diapositive 10 ;

Imaginez une poubelle qui envoie un signal ou une alerte aux personnes responsables de les vider. On élimine ainsi les risques de débordement et de se déplacer pour rien.

Un dernier exemple ;

Des caméras équipées de logiciels d'analyse vidéo pour détecter les incidents de sécurité ou de circulation.



Source : ChatGPT

Diapositive 11 ;

Certaines caméras peuvent aider dans la détection d'incidents de circulation et avertir plus rapidement les services de sécurité. On peut par la suite mieux informer les autres conducteurs.

Les villes intelligentes doivent donc avoir des **super gardiens informatiques** pour protéger toutes les informations et les appareils contre les cyberpirates.

Source : ChatGPT

Diapositive 12 ;

La cybersécurité est extrêmement importante dans les villes intelligentes. Heureusement, les villes ont des personnes capables d'installer et de sécuriser les appareils de l'Internet des objets (Ido).

Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABS LABOS



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Pour se protéger dans les villes intelligentes, les citoyens doivent ressembler à détectives numériques, utiliser des mots de passe forts et ne jamais partager leurs informations personnelles et sensibles !



Source : ChatGPT

Diapositive 13 ;

Les citoyens et les personnes responsables des villes intelligentes doivent demeurer vigilants et s'assurer de ne pas prendre de risques inutiles et d'utiliser les règles premières de la cybersécurité.

L'avenir des villes intelligentes ?

L'avenir des villes intelligentes va sûrement changer, mais il faudra que les ordinateurs et les robots apprennent à collaborer afin de nous rendre la vie plus facile, plus sûre et plus écologique.

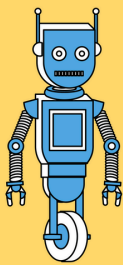


Diapositive 14 ;

Les villes intelligentes utilisent de plus en plus de systèmes connectés, car cela leur permet de réduire certains coûts et ils peuvent mieux encadrer les équipements municipaux. Avec le temps, les villes seront assurément de plus en plus intelligentes.

Les dangers...

Dans les villes intelligentes, il faut faire attention à ce que les ordinateurs et les robots ne deviennent pas méchants et fassent des bêtises !



Source : ChatGPT

Diapositive 15 ;

Certaines personnes ont un peu peur des villes intelligentes. Il est important de s'assurer que les bonnes décisions soient prises et que les systèmes connectés soient installés de manière sécuritaire selon les règles de la cybersécurité.

Heureusement, plusieurs personnes travaillent dans le domaine de la cybersécurité et veillent à nous protéger en tout temps !



Diapositive 16 ;

Plusieurs nouveaux emplois dans le domaine de la cybersécurité sont créés et permettent de s'assurer que tous ces systèmes demeurent cybersécuritaires.



Soyez cyber-chouette!

Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABS LABOS
Créatifs



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Leçon # 10

Les villes intelligentes
peuvent offrir des
avantages, mais
également des
risques.



Diapositive 17 ;

C'est la leçon à retenir. Il est important de demeurer vigilant avec le développement des villes intelligentes autant pour les citoyens que pour les personnes responsables des services informatiques de ces municipalités.

Soyez cyber-chouette!



Diapositive 18 ;

"Soyez cyber-chouette" fait référence à l'animal "une chouette" qui a beaucoup d'intuition, d'intelligence et de sagesse. L'expression "être chouette" signifie le fait d'être joli élégant et digne d'admiration.

Soyez cyber-chouette !

Prochaine leçon :
Travailler en cybersécurité

Diapositive 19 ;

La leçon # 11 portera sur les types d'emplois et sur les possibilités pour ceux ou celles qui veulent travailler dans le domaine de la cybersécurité.



Diapositive 20 ;

Labos créatifs est un organisme sans but lucratif qui aide les écoles à développer une culture de la créativité et d'innovation. Leur site web est ;
<https://www.laboscreatifs.ca/>



Leçon # 10

Apprendre à se protéger
pour les élèves du primaire

Les villes intelligentes
peuvent offrir des avantages
mais aussi des risques.

LABOS
LABOS
LABOS



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Sites Web utiles pour la leçon # 10

Avertissement : Nous utilisons des hyperliens provenant de différentes sources sur internet. Certaines publicités s'y retrouvent sûrement. Avant d'utiliser un hyperlien en classe, il est essentiel de prendre un moment pour le vérifier en privé afin de vous assurer que celui-ci est utilisable en classe avec vos élèves. Nous l'avons vérifié avant de vous le suggérer, mais il est possible qu'avec le temps, le contenu ait été redirigé, modifié ou éliminé. Il est même possible que certaines publicités aient été modifiées et que celles-ci vous rendent inconfortable. Au final, c'est à vous de décider si vous voulez utiliser ou non un hyperlien en salle de classe avec vos élèves. Nous préférons vous en avertir.

- | **Labo créatif** | Lien officiel de l'organisme | Site Web ; <https://www.laboscreatifs.ca/>
- | **Labo créatif** | **Liens francophones pour éduquer à la cybersécurité** | Site Web ; <https://www.laboscreatifs.ca/cybersecurite-ressources>
- | **HabiloMédias** | **La section Cybersécurité d'HabiloMédias** | Site Web ; <https://habilomedias.ca/litteratie-numerique-et-education-aux-medias/enjeux-numeriques/cybersécurité>
- | **Big Bang Science** | **La ville intelligente** | Vidéo YouTube ; <https://youtu.be/qBMUKP5sdJI>
- | **Demain la ville** | **La smart city est morte, vive la smart city!** | Vidéo YouTube ; <https://youtu.be/WEB9nmfPsv8>
- | **Orange** | **Smart City : 60 secondes pour comprendre** | Vidéo YouTube ; <https://youtu.be/-itOe4WjVe4>
- | **CCTV Le Journal** | **Bonjour la Chine | Villes intelligentes du monde** | Vidéo YouTube ; <https://youtu.be/YIGSNjTrxb4>
- | **AFP** | **Santander, la "ville intelligente" la plus connectée d'Europe** | Vidéo YouTube ; <https://youtu.be/DtILnvV-J5A>
- | **Le Devoir** | **Ville intelligente, ville durable ?** | Article de presse ; <https://www.ledevoir.com/societe/science/588631/ville-intelligente-ville-durable>
- | **Asialist (entreprise privée)** | **Les 6 piliers d'une Smart City** | Infographie ; <https://asialyst.com/fr/wp-content/uploads/2016/02/SCHEMA-ASIE-PILIERS-SMART-CITIES-1280x853.jpg>
- | **Journal de Québec** | **De l'eau contaminée par un pirate informatique** | Article de presse ; <https://www.journaldequebec.com/2021/02/08/floride-un-reseau-deau-potable-contamine-par-piratage-informatique>



Leçon # 10 : Les villes intelligentes peuvent offrir des avantages, mais aussi des risques.



Suggestions d'activités complémentaires

Ces activités peuvent être modifiées et adaptées selon l'âge de vos élèves. L'important ici, c'est d'essayer de faire des transferts avec la leçon.

- Réaliser une maquette d'une ville intelligente avec des objets ressemblant à des maisons, des rues, des voitures ou autres démontrant le fonctionnement d'une ville intelligente en respectant les règles premières de la cybersécurité. Soyez créatifs !
- Préparer des affiches avec des conseils sur les bonnes façons de demeurer vigilant dans les villes intelligentes.
- Tenir à jour une liste de mots importants ou créer votre propre glossaire de la cybersécurité.
- Faire une entrevue avec un expert de l'informatique ou un responsable de votre municipalité au sujet des objets connectés utilisés par celle-ci.
- Trouver des statistiques sur les villes intelligentes à partir de sites reconnus.
- Proposer à la direction de votre école, la création d'une brigade de la cybersécurité afin d'aider d'autres élèves et de leur apprendre à mieux se protéger au niveau de la cybersécurité.
- Créer une histoire avec une aventure en cybersécurité.
- Faire une courte présentation à une autre classe de ce que vous avez appris au sujet des villes intelligentes et des moyens pour se protéger.
- Inventer un jeu questionnaire sur les villes intelligentes.
- Créer une courte vidéo pour enseigner comment les villes intelligentes fonctionnent.
- Créer une campagne de sensibilisation en préparant des affiches et placez celles-ci un peu partout dans votre école.
- Inventer un super-héros de la cybersécurité pour votre classe et inventez des histoires que vous pourrez écrire sous forme de livrets avec vos propres dessins.
- Créer une petite pièce et la jouer avec un théâtre de marionnettes.
- Utilisez "cyber-chouette" pour créer et résoudre des problèmes de mathématiques ou pour écrire des histoires de détectives qui partent en mission.
- Organiser un concours avec des slogans de protection en cybersécurité.



Soyez cyber-chouette!

Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



Objectif de cette leçon

Dans la leçon # 11, les élèves apprendront qu'il existe plusieurs types de métiers reliés à la cybersécurité et que c'est un domaine en forte demande avec de bons salaires et de belles opportunités pour y travailler.

Démarche proposée

Nous vous suggérons tout simplement de prendre un moment dans la journée pour passer en revue les différentes diapositives de la leçon # 11 et d'avoir une discussion avec vos élèves concernant les pièges de la cybersécurité. Il n'est pas nécessaire d'avoir de grandes connaissances dans le domaine. Grâce aux diapositives de la leçon # 11 du programme "Soyez cyber-chouette !" comme support pédagogique, vous pourrez facilement présenter de nouveaux concepts et des mots importants ainsi que le jargon du monde de la cybersécurité. L'important ici sera de prendre un temps d'arrêt et d'avoir cette discussion unique et essentielle avec vos élèves.

Questions d'objectivation

Voici quelques exemples de questions d'objectivations qui pourraient être utiles pendant ou après avoir visionné la leçon. N'hésitez pas à les modifier ou à y ajouter vos propres questions au besoin ;

- **Élèves de la maternelle à la 3^e année ;**
 - Connaissez-vous des personnes qui travaillent avec les ordinateurs ?
 - Avez-vous des exemples de métiers qui servent à protéger les personnes sur Internet ?
 - Est-ce que ces métiers sont importants ? Pourquoi ?
- **Élèves de 4^e à la 6^e année ;**
 - Connaissez-vous des personnes qui travaillent dans le domaine de la cybersécurité ?
 - Quels seraient, selon vous, des exemples de métiers essentiels pour nous protéger sur Internet ou lorsqu'on utilise des appareils informatiques ?
 - Est-ce que ces métiers sont essentiels ? Pourquoi ?
 - Est-ce que ces métiers sont nombreux et différents, pourquoi ?
 - Est-ce un métier qui pourrait vous intéresser ? Pourquoi ?



Soyez cyber-chouette!



Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABOS
LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



Soyez cyber-chouette!

Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABOS
LABOS



Diapositive 1 ;

L'objectif de la leçon # 11 est de comprendre qu'il existe plusieurs types de métiers liés à la cybersécurité et que c'est un domaine en forte demande avec de bons salaires et de belles opportunités pour y travailler.

Diapositive 2 ;

On peut commencer par une question ouverte et voir ce que les élèves savent déjà à ce sujet.



Quels sont les métiers de la cybersécurité ?

Les personnes qui travaillent en cybersécurité sont comme des super-héros de l'informatique qui protègent les ordinateurs et les données des attaques des cyberpirates sur Internet.



Source : ChatGPT

Diapositive 3 ;

Souvent, lorsqu'il y a des désagréments en informatique, les personnes qui travaillent dans ce domaine sont appelés en renforts et donnent un sérieux coup de pouce à plusieurs personnes.

Celles et ceux qui travaillent dans le domaine de la cybersécurité, vont prendre les moyens pour détecter et faire arrêter les pirates informatiques. Ils vont sécuriser les sites web pour éviter les attaques, et protéger les informations personnelles et sensibles des personnes.



Source : ChatGPT

Diapositive 4 ;

Généralement, les personnes qui travaillent dans le domaine de la cybersécurité, s'assurent que les sites web sont sécuritaires et ils protègent nos informations personnelles et sensibles. Ils mettent en place des systèmes pour détecter et arrêter les pirates informatiques.



Soyez cyber-chouette!



Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



Est-ce que travailler en cybersécurité est une bonne idée ?

Diapositive 5 ;

Avant de passer à la prochaine diapositive, vous pouvez demander aux élèves de répondre à cette question. Est-ce qu'il y en a parmi eux qui aimeraient faire ce genre de travail ? Pourquoi ?



Il y existe toutes sortes d'emplois possibles dans plusieurs domaines de la cybersécurité.

Diapositive 6 ;

Il existe plusieurs types d'emplois en cybersécurité. Ces emplois changent avec le temps et d'autres s'ajoutent selon les nouveaux développements en informatique et les besoins grandissants en cybersécurité.



Travailler en cybersécurité n'est pas toujours facile.

Diapositive 7 ;

Travailler en cybersécurité n'est pas toujours facile et il faut compléter des études selon le type d'emplois qu'on veut occuper. Il faut toujours continuer à s'informer et à apprendre. au sujet des nouvelles façons de faire.

Il faut savoir comment résoudre des problèmes, mais c'est un secteur avec beaucoup de possibilités.



Diapositive 8 ;

Les plus grands défis de celles et ceux qui travaillent dans ce domaine restent la capacité à comprendre et à résoudre des problèmes. Il y a beaucoup d'emplois qui en général peuvent être bien rémunérés.



Soyez cyber-chouette!



Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABS LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



On retrouve les chapeaux noirs et les chapeaux blancs. Les chapeaux noirs sont les pirates et les criminels des réseaux informatiques.



Diapositive 9 ;

Dans le jargon de la cybersécurité, "les chapeaux noirs" font référence aux cyberpirates et aux criminels de la cybersécurité.



Les chapeaux blancs, en revanche, sont celles et ceux qui protègent les réseaux informatiques et aident les personnes à ne pas tomber dans les pièges.

Diapositive 10 ;

Dans le jargon de la cybersécurité, "les chapeaux blancs" sont celles et ceux qui font le bien et qui aident les personnes à se protéger. Dans le domaine de la cybersécurité, ce sont les chapeaux blancs qui sont recherchés pour travailler.

Il existe plusieurs types d'emplois en cybersécurité.

Responsable de la cybersécurité

Ingénieur

Architecte de réseau

Testeur de réseau

Consultant en sécurité

Analyste

Source : ChatGPT

Diapositive 11 ;

Il existe des dizaines de sortes de métiers et de types d'emplois en cybersécurité. Cela change d'années en années. En voici quelques exemples...

L'important, c'est de se rappeler qu'il est possible de travailler en cybersécurité



Diapositive 12 ;

Ici, l'important n'est pas de se rappeler toutes ces informations par cœur. On veut seulement faire réaliser qu'il y existe plusieurs types d'emplois pour les garçons et les filles qui sont intéressés par le domaine de la cybersécurité.



Soyez cyber-chouette!



Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABS LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



La cybersécurité est un domaine en forte croissance et il manque déjà plusieurs travailleurs qualifiés.



Source : ChatGPT

Diapositive 13 ;

La cybersécurité change constamment et il y a une forte demande dans le domaine un peu partout sur la planète.

L'avenir de la cybersécurité ?

La cybersécurité est un domaine important qui continue de changer et qui peut être très passionnant autant pour les filles que les garçons.



Diapositive 14 ;

Les nombreuses avancées dans le domaine de l'informatique et les besoins grandissants en cybersécurité garantissent qu'il y a plusieurs emplois disponibles et très bien rémunérés.

Soyez un chapeau blanc de la cybersécurité !



Diapositive 15 ;

On encourage les jeunes à faire le bien lorsqu'ils ou elles utilisent l'internet, les réseaux sociaux ou les outils de la cybersécurité. Nous avons tous un rôle à jouer.

Heureusement, apprendre à travailler en cybersécurité est possible et les emplois sont nombreux et divers.



Diapositive 16 ;

Il existe plusieurs programmes de formation en cybersécurité, que ce soit dans les collèges et universités de sa province ou ailleurs.



Soyez cyber-chouette!

Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABS LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



Leçon # 11

Il y a beaucoup de
métiers à
découvrir en
cybersécurité.



Diapositive 17 ;

C'est la leçon à retenir. Il y a beaucoup de métiers différents et possibles dans le domaine de la cybersécurité.

Soyez cyber-chouette!



Diapositive 18 ;

"Soyez cyber-chouette" fait référence à l'animal "une chouette" qui a beaucoup d'intuition, d'intelligence et de sagesse. L'expression "être chouette" signifie le fait d'être joli élégant et digne d'admiration.

Soyez cyber-chouette !

Prochaine leçon :
12 conseils à retenir pour devenir
cyber-chouette en cybersécurité

Diapositive 19 ;

La leçon # 12 présentera la cybersécurité dans son ensemble et sera un résumé des leçons # 1 à 11.



Diapositive 20 ;

Labos créatifs est un organisme sans but lucratif qui aide les écoles à développer une culture de la créativité et d'innovation. Leur site web est ;
<https://www.laboscreatifs.ca/>



Soyez cyber-chouette!

Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABOS
LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



Sites Web utiles pour la leçon # 11 ;

Avertissement : Nous utilisons des hyperliens provenant de différentes sources sur internet. Certaines publicités s'y retrouvent sûrement. Avant d'utiliser un hyperlien en classe, il est essentiel de prendre un moment pour le vérifier en privé afin de vous assurer que celui-ci est utilisable en classe avec vos élèves. Nous l'avons vérifié avant de vous le suggérer, mais il est possible qu'avec le temps, le contenu ait été redirigé, modifié ou éliminé. Il est même possible que certaines publicités aient été modifiées et que celles-ci vous rendent inconfortable. Au final, c'est à vous de décider si vous voulez utiliser ou non un hyperlien en salle de classe avec vos élèves. Nous préférons vous en avertir.

- | **Labo créatif** | Lien officiel de l'organisme | Site Web ; <https://www.laboscreatifs.ca/>
- | **Labo créatif** | **Liens francophones pour éduquer à la cybersécurité** | Site Web ; <https://www.laboscreatifs.ca/cybersecurite-ressources>
- | **HabiloMédias** | Lien officiel de l'organisme | Site Web ; Site web du Centre canadien d'éducation aux médias et de littératie numérique ; <http://habilomedias.ca/>
- | **HabiloMédias** | **La section Cybersécurité d'HabiloMédias** | Site Web ; <https://habilomedias.ca/litteratie-numerique-et-education-aux-medias/enjeux-numeriques/cybersécurité>
- | **La Provence** | **Les "white hats", ces hackers qui vous veulent du bien** | Article de presse ; <https://www.laprovence.com/article/societe/5596830/les-white-hackers-ces-pirates-qui-vous-veulent-du-bien.html>
- | **Kaspersky (entreprise privée)** | **Chapeaux noirs, chapeaux blancs et chapeaux gris : définition et explication** | Article web ; <https://www.kaspersky.fr/resource-center/definitions/hacker-hat-types>
- | **Michel Kartner** | **Les 15 métiers de la cybersécurité : Guide complet** | Vidéo YouTube ; <https://youtu.be/W8GNMNQn2Fo>
- | **Michel Kartner** | **Top 10 des compétences en cybersécurité : 100 offres d'emploi analysées** | Vidéo YouTube ; <https://youtu.be/vuGIBGna-RI>
- | **CEA Recherche** | **Michaël, ingénieur-chercheur en cybersécurité** | Vidéo YouTube ; <https://youtu.be/RYxd-xPGiZM>
- | **IMS Networks** | **Qu'est-ce qu'un SOC (Security Operations Center) ? - 5 minutes pour comprendre** | Vidéo YouTube ; <https://youtu.be/Awsajwvlris>
- | **1 jour 1 question** | **C'est quoi une cyberattaque ?** | Vidéo YouTube ; <https://youtu.be/nTs1kv4N6nl>
- | **RTI Officiel** | **2 minutes pour comprendre la cybersécurité** | Vidéo YouTube ; <https://youtu.be/S1kNXCdMgVI>
- | **Monsieur Techno** | **Les réseaux informatiques et Internet** | Vidéo YouTube ; <https://www.youtube.com/watch?v=JqweQE6TDTc>



Soyez cyber-chouette!

Leçon # 11

Apprendre à se protéger
pour les élèves du primaire

Il y a beaucoup de métiers à
découvrir en cybersécurité!

LABS LABOS



Leçon # 11 : Il y a beaucoup de métiers à découvrir en cybersécurité.



Suggestions d'activités complémentaires

Ces activités peuvent être modifiées et adaptées selon l'âge de vos élèves. L'important ici, c'est d'essayer de faire des transferts avec la leçon.

- Réaliser un petit sondage sur les métiers en cybersécurité en général et pour savoir si les personnes les connaissant déjà ou non.
- Préparer des affiches avec des descriptions de métiers dans le domaine de la cybersécurité.
- Tenir à jour une liste de mots importants ou créer votre propre glossaire de la cybersécurité.
- Faire une entrevue avec une personne qui travaille dans le domaine de la cybersécurité.
- Trouver des statistiques sur les différents métiers de la cybersécurité à travers le pays ou de la planète.
- Créer une histoire avec une aventure en cybersécurité.
- Faire une courte présentation à une autre classe de ce que vous avez appris au sujet des métiers possibles en cybersécurité.
- Inventer un jeu questionnaire de la cybersécurité et sur les différents métiers dans le domaine de la cybersécurité.
- Créer une courte vidéo pour expliquer différents métiers dans le domaine de la cybersécurité.
- Proposer à la direction de votre école, la création d'une brigade de la cybersécurité afin d'aider d'autres élèves et de leur apprendre à mieux se protéger au niveau de la cybersécurité.
- Créer une campagne de sensibilisation en préparant des affiches et placez celles-ci un peu partout dans votre école.
- Inventer un super-héros de la cybersécurité pour votre classe et inventez des histoires que vous pourrez écrire sous forme de livrets avec vos propres dessins.
- Créer une petite pièce et la jouer avec un théâtre de marionnettes.
- Utilisez "cyber-chouette" pour créer et résoudre des problèmes de mathématiques ou pour écrire des histoires de détectives qui partent en mission.
- Écrire une lettre à ses parents ou à des membres de sa famille qui explique les meilleures façons de se protéger les éléments de sa vie privée.



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABS LABOS



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Objectif de cette leçon

La leçon # 12 sera l'occasion pour revoir et pour faire un résumé de toutes les autres leçons depuis le tout début. Nous allons transformer les 12 leçons et les convertir en 12 conseils à retenir pour devenir "cyber-chouette" en cybersécurité.

Démarche proposée

Nous vous suggérons tout simplement de prendre un moment dans la journée et présenter les diapositives de la leçon 12 avec vos élèves. Les diapositives présentent les "**12 conseils à retenir pour devenir cyber-chouette en cybersécurité**". Nous vous suggérons tout de prendre un moment avec vos élèves pour revoir les 12 conseils et pour faire un retour sur les leçons # 1 à 12. Demandez aux élèves s'ils se rappellent des leçons en passant d'une diapositive à l'autre. Ils peuvent, par exemple, expliquer ce qu'ils ont appris et donner des exemples et expliquer l'importance d'apprendre à se protéger en cybersécurité. Vous pouvez, en terminant, suggérer à vos élèves de réaliser certaines activités proposées lors des dernières leçons ou devenir des passeurs de la cybersécurité, et ainsi à assister à d'autres élèves de votre école et de mettre en pratique ce qu'ils auront appris.

Questions d'objectivation

Voici quelques exemples de questions d'objectivations qui pourraient être utiles pendant ou après avoir visionné la leçon # 12. N'hésitez pas à les modifier ou à y ajouter vos propres questions au besoin ;

- **Élèves de la maternelle à la 6^e année ;**
 - Avez-vous aimé ces leçons au sujet de la cybersécurité ? Pourquoi ?
 - Est-ce important ?
 - Est-ce qu'il y a quelque chose d'autres que vous souhaiteriez apprendre ou faire avec la cybersécurité ?
 - Est-qu'il y a quelque chose que nous pourrions faire pour aider d'autres élèves ou des personnes de notre communauté ?
 - Avez-vous des choses que vous aimeriez connaître plus en détail ?
 - Quel conseil semble être le plus important ? Pourquoi ?



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABOS
LABOS
Céa



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Soyez cyber-chouette!

Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABOS
LABOS
Céa



Diapositive 1 ;

L'objectif de la leçon 12 est de faire le résumé de toutes les leçons apprises depuis le tout début et de présenter une liste de 12 conseils à retenir pour devenir *cyber-chouette* en cybersécurité.

Diapositive 2 ;

La leçon vous permettra de revoir les concepts présentés tout au long des leçons depuis le début.



Voici un petit résumé de
toutes nos leçons...

Diapositive 3 ;

Il sera important de bien ajuster le temps des discussions selon l'âge et l'intérêt des élèves. Il y a ici beaucoup de matière à discuter et à revoir. Vous pouvez faire cette leçon en plusieurs étapes si vous le désirez.



Diapositive 4 ;

Les leçons se sont transformées, un peu par magie, en 12 conseils à retenir pour devenir *cyber-chouette* en cybersécurité.



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABS LABOS



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Conseil # 1

Il est important
d'apprendre à ne pas
tomber dans les pièges
de la cybersécurité.



Diapositive 5 ;

Le premier conseil est de comprendre qu'il est important de ne pas tomber dans les pièges et les vulnérabilités qui pourraient nous piéger. Demander aux élèves d'expliquer pourquoi c'est essentiel.

Conseil # 2

Il faut toujours utiliser
un mot de passe
robuste.



Diapositive 6 ;

Revoir avec les élèves entre un mot de passe faible et un mot de passe fort. Demander leur pourquoi ceci est important.

Conseil # 3

L'hameçonnage, ne
pas se faire attraper
comme un poisson.



Diapositive 7 ;

C'est une belle occasion pour revoir les techniques et la définition de l'hameçonnage. Demander aux élèves pourquoi c'est important.

Conseil # 4

Les maliciels, apprenez
ce qu'ils sont et ce
qu'ils font.



Diapositive 8 ;

Les maliciels sont souvent installés à la suite d'une attaque par hameçonnage. Demander aux élèves ce que sont les maliciels et ce qu'ils font.



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABOS
LABOS



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Conseil # 5

Protégeons notre vie
privée ; ne soyons pas
un livre ouvert.



Diapositive 9 ;

Il est important de se rappeler qu'il ne faut jamais partager nos informations personnelles ou sensibles. Demandez aux élèves d'expliquer la différence entre ces deux types d'informations et d'expliquer pourquoi cela est essentiel.

Conseil # 6

Les réseaux sociaux ;
Il vaut mieux réfléchir
pour se protéger.



Diapositive 10 ;

Les réseaux sociaux sont des endroits où des personnes peuvent publier des informations personnelles ou sensibles. Il est essentiel de bien réfléchir avant de choisir ce que l'on veut partager. Demander aux élèves pourquoi cela est important ?

Conseil # 7

L'ingénierie sociale est
un autre type de piège
de la cybersécurité.



Diapositive 11 ;

L'ingénierie sociale est tout simplement un autre type de piège en cybersécurité où les pirates essaient de nous faire prendre de mauvaises décisions, souvent rapidement et sans vraiment prendre un moment pour réfléchir.

Conseil # 8

L'internet des objets (Ido),
il est important de
connaître les risques.



Diapositive 12 ;

L'internet des objets peut être utile pour nous simplifier la vie, mais les objets connectés sont des portes d'entrées pour les pirates informatiques. Les objets connectés doivent être sécurisés et fiables.



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABS LABOS



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Conseil # 9

L'intelligence artificielle (IA),
il faut faire attention aux
hallucinations.



Diapositive 13 ;

L'Intelligence artificielle (IA) peut nous faciliter la vie, mais il arrive à l'occasion de voir des hallucinations d'IA qui sont en fait des erreurs ou des fausses informations. Il est essentiel de demeurer vigilant et de toujours prendre un moment pour vérifier nos informations.

Conseil # 10

Les villes intelligentes
peuvent offrir des avantages
mais également des risques.



Diapositive 14 ;

Les villes intelligentes peuvent permettre à une meilleure qualité de vie, plus de sécurité et nous aider à protéger l'environnement. Il faut quand même s'assurer que les villes intelligentes soient sécurisées au niveau de la cybersécurité.

Conseil # 11

Il y a beaucoup de
métiers à découvrir
en cybersécurité.



Diapositive 15 ;

Plusieurs nouveaux emplois existent dans plusieurs domaines de la cybersécurité. Il y a aussi présentement une forte demande pour des personnes qualifiées et intéressées par ce domaine.

Et pour terminer...



Diapositive 16 ;

Et, maintenant, voici un dernier conseil pour conclure cette leçon...



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABS LABOS
Créatifs



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Conseil # 12

Avec la cybersécurité, il
faut toujours demeurer
vigilant et continuer à
apprendre.



Diapositive 17 ;

C'est la leçon à retenir. Il est important de toujours demeurer vigilant et se souvenir que les technologies vont changer avec le temps. Il est essentiel de continuer à apprendre à s'informer sur l'évolution de la cybersécurité et de connaître les meilleurs moyens pour se protéger.

Ces 12 conseils
sont super
importants afin de
mieux se protéger!



Diapositive 18 ;

Nous avons créé deux affiches à la fin de ce document que vous pourrez placer un peu partout dans votre classe ou dans l'école. Ces conseils vont aider les élèves à retenir ce qu'il faut faire pour mieux se protéger.

Bravo, vous êtes
cyber-chouette !



Diapositive 19 ;

Bravo pour votre persévérance et pour avoir pris le temps de mieux éduquer vos élèves à la cybersécurité. Chez Labos Créatifs, nous offrons d'autres ressources en cybersécurité. N'hésitez pas à nous contacter au besoin.

Diapositive 20 ;

Labos créatifs est un organisme sans but lucratif qui aide les écoles à développer une culture de la créativité et d'innovation. Leur site web est ;
<https://www.laboscreatifs.ca/>



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABOS
LABOS
créatifs



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Sites Web utiles pour la leçon # 12 ;

Avertissement : Nous utilisons des hyperliens provenant de différentes sources sur internet. Certaines publicités s'y retrouvent sûrement. Avant d'utiliser un hyperlien en classe, il est essentiel de prendre un moment pour le vérifier en privé afin de vous assurer que celui-ci est utilisable en classe avec vos élèves. Nous l'avons vérifié avant de vous le suggérer, mais il est possible qu'avec le temps, le contenu ait été redirigé, modifié ou éliminé. Il est même possible que certaines publicités aient été modifiées et que celles-ci vous rendent inconfortable. Au final, c'est à vous de décider si vous voulez utiliser ou non un hyperlien en salle de classe avec vos élèves. Nous préférons vous en avertir.

- | **Labo créatif** | Lien officiel de l'organisme | Site Web ; <https://www.laboscreatifs.ca/>
- | **Labo créatif** | **Liens francophones pour éduquer à la cybersécurité** | Site Web ; <https://www.laboscreatifs.ca/cybersecurite-ressources>
- | **HabiloMédias** | **La section Cybersécurité d'HabiloMédias** | Site Web ; <https://habilomedias.ca/litteratie-numerique-et-education-aux-medias/enjeux-numeriques/cybersécurité>
- | **HabiloMédias** | **Les enjeux pour les jeunes enfants** | Site Web ; <https://habilomedias.ca/cybersecurite/cybersecurite-enjeux-jeunes-enfants>
- | **HabiloMédias** | **Les enjeux pour les adolescents** | Site Web ; <https://habilomedias.ca/litteratie-numerique-et-education-aux-medias/enjeux-numeriques/cybersécurité/cybersécurité-les-enjeux-pour-les-adolescents>
- | **Gouvernement du Canada** | **Pensez Cybersécurité** | Site web ; <https://www.pensezcybersecurite.gc.ca/index-fr.aspx>
- | **Gendarmerie royale du Canada** | **Centre de prévention du crime chez les jeunes** | Site web ; <https://www.rcmp-grc.gc.ca/fr/securite-des-jeunes/centre-de-prevention-du-crime-chez-les-jeunes>
- | **Enfants Avertis** | Site web ; <https://www.kidsintheknow.ca/app/fr/about>
- | **AidezMoiSVP** | Site web ; <https://needhelponow.ca/app/fr/>
- | **CyberJulie** | Site web ; <http://cyberjulie.ca/app/fr/>
- | **Centre canadien de la protection de l'enfance** | Site web ; <https://protectchildren.ca/fr/>
- | **Centre canadien de protection de l'enfance** | **Ressource éducative gratuites** | Site web ; https://www.kidsintheknow.ca/app/fr/parents-educational_tools
- | **Centre canadien de protection de l'enfance** | **Projet Arachnid** | Site web ; <https://protegeonsnosenfants.ca/fr/programmes-et-initiatives/projet-arachnid/>
- | **Te fais pas sextorquer** | Site web ; <https://tefaispassextorquer.ca/>
- | **Parents Cyberavertis.ca** | Site web ; <https://parents cyberavertis.ca/app/fr/>



Leçon # 12

Apprendre à se protéger
pour les élèves du primaire

12 conseils à retenir pour
devenir cyber-chouette
en cybersécurité.

LABOS
LABOS



Leçon # 12 : Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.



Suggestions d'activités complémentaires

Ces activités peuvent être modifiées et adaptées selon l'âge de vos élèves. L'important ici, c'est d'essayer de faire des transferts avec la leçon.

- Réaliser un petit sondage sur la cybersécurité en général et sur l'utilisation des réseaux sociaux par les élèves ou les adultes de l'école.
- Préparer des affiches avec des conseils sur les bonnes façons d'utiliser les réseaux sociaux.
- Tenir à jour une liste de mots importants ou créer votre propre glossaire de la cybersécurité.
- Faire une entrevue avec un expert de l'informatique.
- Trouver des statistiques sur les problèmes reliés à la cybersécurité en général.
- Créer une histoire avec une aventure en cybersécurité.
- Faire une courte présentation à une autre classe de ce que vous avez appris au sujet de l'utilisation des réseaux sociaux et des moyens pour se protéger.
- Inventer un jeu questionnaire de la cybersécurité sur l'utilisation des réseaux sociaux.
- Créer une courte vidéo pour enseigner les risques de l'utilisation des réseaux sociaux et donner des trucs pour se protéger.
- Proposer à la direction de votre école, la création d'une brigade de la cybersécurité afin d'aider d'autres élèves et de leur apprendre à mieux se protéger au niveau de la cybersécurité.
- Créer une campagne de sensibilisation en préparant des affiches et placez celles-ci un peu partout dans votre école.
- Inventer un super-héros de la cybersécurité pour votre classe et inventez des histoires que vous pourrez écrire sous forme de livrets avec vos propres dessins.
- Créer une petite pièce et la jouer avec un théâtre de marionnettes.
- Utilisez "cyber-chouette" pour créer et résoudre des problèmes de mathématiques ou pour écrire des histoires de détectives qui partent en mission.
- Écrire une lettre à ses parents ou à des membres de sa famille qui explique les meilleures façons de se protéger lorsqu'ils utilisent les réseaux sociaux.
- Organiser un concours avec des slogans de protection en cybersécurité.



Conclusion et remerciements



Nous aimerions vous remercier d'avoir bien voulu prendre un moment et utiliser notre recueil d'activités pour les élèves du primaire.

Labos Créatifs est un organisme sans but lucratif situé au Canada atlantique. Nous encourageons l'apprentissage pratique et expérimental qui permet aux jeunes de développer leur apprentissage par l'entremise de la créativité, de l'innovation et de la technologie d'aujourd'hui en intégrant les Objectifs de développement durable (ODD) des Nations Unies.

Nous aimerions aussi, en terminant, vous inviter à développer l'esprit d'entreprise dans vos salles de classe et dans vos communautés. N'hésitez pas à nous faire signe au besoin et merci de faire une différence dans les programmes d'enseignement au Canada ou ailleurs.

<https://www.laboscreatifs.ca/>



À propos de l'auteur;

Roberto Gauvin est consultant en éducation chez Édunovis. Il est également chargé de cours à l'Université de Moncton. Roberto est à la retraite en tant qu'éducateur professionnel depuis juin 2020. Il a travaillé plus de trente-six ans dans le domaine de l'éducation en tant qu'enseignant, directeur d'école et consultant. Il était directeur du Centre d'apprentissage du Haut-Madawaska (CAHM), une école francophone de la maternelle à la 8e année située à Clair au Nouveau-Brunswick, Canada, pendant près de vingt ans. Roberto a également été spécialiste en éducation pendant deux ans avant sa retraite chez CyberNB, un ancien organisme spécial d'Opportunité NB.

<https://edunovis.com/>



Support-visuel # 1

Soyez cyber-chouette!

12 conseils à retenir pour devenir cyber-chouette en cybersécurité



1. Il est important d'apprendre à ne pas tomber dans les pièges des cyberpirates.
2. Il faut toujours utiliser un mot de passe robuste.
3. L'hameçonnage, ne pas se faire attraper comme un poisson.
4. Les maliciels, apprenez ce qu'ils sont et ce qu'ils font.
5. Protégeons notre vie privée ; ne soyons pas un livre ouvert.
6. Les réseaux sociaux ; il vaut mieux réfléchir pour se protéger.
7. L'ingénierie sociale est un autre type de piège de la cybersécurité.
8. L'internet des objets (Ido), il est important de connaître les risques.
9. L'intelligence artificielle (IA), il faut faire attention aux hallucinations.
10. Les villes intelligentes peuvent offrir des avantages, mais également des risques.
11. Il y a beaucoup de métiers à découvrir en cybersécurité.
12. Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.

Support-visuel # 2

Soyez cyber-chouette!

12 conseils à retenir pour devenir cyber-chouette en cybersécurité

Il faut toujours utiliser un mot de passe robuste.

Il est important d'apprendre à ne pas tomber dans les pièges des cyberpirates.

Protégeons notre vie privée ; ne soyons pas un livre ouvert.

L'hameçonnage, ne pas se faire attraper comme un poisson.

Les malicieux, apprenez ce qu'ils sont et ce qu'ils font.

Les réseaux sociaux ; il vaut mieux réfléchir pour se protéger.

L'ingénierie sociale est un autre type de piège de la cybersécurité.

Avec la cybersécurité, il faut toujours demeurer vigilant et continuer à apprendre.

L'internet des objets (Ido), il est important de connaître les risques.

L'intelligence artificielle (IA), il faut faire attention aux hallucinations.

Il y a beaucoup de métiers à découvrir en cybersécurité.

Les villes intelligentes peuvent offrir des avantages mais également des risques.