

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Trousse de ressources pédagogiques Novembre 2020

AVANT-PROPOS

La publication intitulée *Trousse de ressources pédagogiques* est un document NON CLASSIFIÉ qui présente de nombreuses ressources pouvant aider les enseignants à favoriser l'apprentissage dans le domaine de la cybersécurité et des technologies de l'information. Cette publication n'a pas pour but de recommander des ressources; elle vise plutôt à présenter diverses sources susceptibles d'appuyer le cheminement de carrière en cybersécurité.

Avertissement : Les ressources figurant dans le présent document ne sont ni validées ni recommandées par le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications. L'information fournie se veut un résumé général des renseignements accessibles publiquement.

HISTORIQUE DES MODIFICATIONS

| Version | Modifications | Date |
|---------|-------------------|---------------|
| 1 | Première version. | Novembre 2020 |
| | | |
| | | |
| | | |

TABLE DES MATIÈRES

| | | |
|----------|---|-----------|
| 1 | Introduction | 4 |
| 1.1 | Centre canadien pour la cybersécurité | 4 |
| 1.2 | Objet..... | 4 |
| 2 | Ressources pour les cycles primaires et secondaires | 5 |
| 2.1 | De la maternelle à la 6 ^e année | 5 |
| 2.2 | De la 7 ^e à la 12 ^e année (secondaires 1 à 5) | 6 |
| 3 | Ressources postsecondaires | 10 |
| 4 | Ressources gouvernementales | 12 |
| 4.1 | Ressources du gouvernement du Canada | 12 |
| 4.2 | Ressources de pays alliés du Canada..... | 12 |
| 5 | Ressources supplémentaires | 15 |
| 5.1 | Blogues..... | 15 |
| 5.2 | Vidéos et webinaires | 15 |
| 5.3 | Balados..... | 16 |
| 5.4 | Jeux en ligne..... | 17 |

1 INTRODUCTION

La demande de professionnels et de praticiens en cybersécurité ne cesse de croître au Canada et partout dans le monde, et les besoins liés aux curriculums en cybersécurité augmentent à leur tour. Le fait d'avoir acquis des compétences et des connaissances pertinentes dans le domaine peut permettre à un candidat de se démarquer des autres. Les organisations sont à la recherche de candidats talentueux qui ont reçu une formation de qualité supérieure et obtenu de l'expérience pratique.

La trousse de ressources pédagogiques est un outil pratique visant à aider les enseignants et les professeurs à éveiller l'intérêt de leurs étudiants pour la cybersécurité et à permettre à ceux-ci de se familiariser avec de nouveaux outils, des innovations et de nouvelles ressources qui leur permettront d'améliorer leurs connaissances et compétences dans les domaines de la science, de la technologie, de l'ingénierie et des mathématiques (STIM). Elle présente des ressources gouvernementales ainsi que des ressources de l'industrie et du secteur privé pouvant servir aux fins de formation complémentaire et à titre d'information dans le but d'améliorer les connaissances et les compétences d'élèves et d'étudiants de tous les niveaux en STIM, y compris la cybersécurité.

1.1 CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a été mis sur pied en octobre 2018. L'équipe des Relations et de la collaboration avec le milieu universitaire du Centre pour la cybersécurité travaille de concert avec les universités, les collèges, les associations, les comités ministériels à vocation éducative et les professeurs du secteur privé dans le but d'accroître les capacités et le bassin de candidats talentueux en cybersécurité au Canada. L'équipe collabore également avec le personnel enseignant afin d'aider la collectivité à mieux comprendre la cybersécurité. Sa mission consiste à faire du Canada un leader mondial en cybersécurité en renforçant les programmes d'études portant sur le sujet.

1.2 OBJET

Le présent document s'adresse principalement aux enseignants et aux professeurs qui s'apprêtent à donner des programmes axés sur la cybersécurité et les technologies de l'information, ou qui souhaitent ajouter d'autres éléments à leur curriculum. Il permettra également aux étudiants qui s'intéressent à une carrière en cybersécurité de trouver d'autres ressources dans le domaine.

Les ressources figurant dans le présent document ne sont ni validées ni recommandées par le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications. L'information fournie se veut un résumé général des renseignements accessibles publiquement.

Tous les efforts ont été faits pour assurer l'exactitude de l'information, mais compte tenu de la nature dynamique de la cybersécurité, cette trousse sera passée en revue périodiquement afin de tenir les ressources à jour. Les nouvelles ressources ou les modifications proposées peuvent être envoyées par courriel à l'adresse contact@cyber.gc.ca.

2 RESSOURCES POUR LES CYCLES PRIMAIRES ET SECONDAIRES

2.1 DE LA MATERNELLE À LA 6^E ANNÉE

Common Sense Education (en anglais) : Tous les élèves ont besoin de compétences en citoyenneté numérique pour s'engager à fond dans leur communauté et faire des choix judicieux en ligne et dans la vie de tous les jours. Le programme de citoyenneté numérique de la maternelle à la 12^e année a reçu des prix et atteint les objectifs ci-dessous :

- Donner suite aux principales préoccupations en milieu scolaire;
- Préparer les élèves en développant des compétences fondamentales pour le 21^e siècle;
- Appuyer le personnel enseignant par le truchement de la formation et de la reconnaissance;
- Mettre à contribution l'ensemble de la communauté en sensibilisant les familles.

Site Web : <https://www.commonsense.org/education/digital-citizenship/curriculum>

Cybint (en anglais) : À titre d'entreprise mondiale vouée à l'éducation en cybersécurité, Cybint s'engage au recyclage professionnel de l'effectif et à l'amélioration des compétences dans l'industrie de la cybersécurité. Cybint offre des solutions novatrices de pointe en matière d'éducation et de formation pour contrer les deux grandes menaces qui pèsent sur le domaine de la cybersécurité : la pénurie de talents et les lacunes dans les compétences.

Site Web : <https://www.cybintsolutions.com/about/>

Animation Scratch : Scratch est spécialement conçu pour les enfants de 8 à 16 ans, mais il est utilisé par des personnes de tous les âges. Des millions de gens créent des projets avec Scratch dans un large éventail de situations, y compris les maisons, les écoles, les musées, les bibliothèques et les centres communautaires. Les élèves peuvent utiliser Scratch pour programmer leurs propres histoires interactives, animations et jeux. En même temps, ils apprennent à penser de façon créative et à travailler ensemble – des compétences essentielles pour tout le monde dans la société actuelle. Les éducateurs intègrent Scratch dans différents domaines et groupes d'âge.

Site Web : <https://scratch.mit.edu/projects/editor/?tutorial=getStarted>

Kids Code Jeunesse : Kids Code Jeunesse (kcj) est un organisme de bienfaisance canadienne bilingue, déterminé à donner à chaque enfant canadien l'accès à une éducation aux compétences numériques, en mettant l'accent sur les filles et les communautés insuffisamment desservies. Il cherche à favoriser le développement de la pensée informatique chez tous les enfants du Canada dans le cadre du codage.

Site Web : <https://kidscodejeunesse.org/fr/accueil>

Code Club : Code Club Canada est un réseau national de bénévoles et d'instructeurs qui dirigent des clubs de codage gratuits pour les enfants âgés de 8 à 12 ans afin de leur permettre d'apprendre à développer et à partager leurs idées tout en acquérant des connaissances. Les clubs se tiennent dans les écoles, les bibliothèques et les centres communautaires et durent 8 semaines.

Site Web : <https://codeclub.ca/fr/accueil.html>

L'éducation à la citoyenneté numérique dans les écoles de la Saskatchewan : L'éducation à la citoyenneté numérique dans les écoles de la Saskatchewan est un guide pour les responsables des divisions scolaires qui travaillent avec les administrateurs scolaires et les enseignants pour aider les élèves à acquérir une compréhension du comportement en ligne sûr et approprié. Le guide propose une feuille de route pour développer des politiques de citoyenneté numérique à l'échelle de la division scolaire ainsi que des lignes directrices et des procédures dans les écoles. Il offre des outils et des ressources pour soutenir l'éducation à la citoyenneté numérique et un continuum de citoyenneté numérique pour les élèves de la maternelle à la 12^e année.

Site Web : <https://bekindonline.com/wp-content/uploads/2019/02/leducation-a-la-citoyennete-numerique-dans-les-ecoles-de-la-saskatchewan.pdf>

Technovation : Technovation est un organisme international à but non lucratif à vocation pédagogique qui encourage les filles et les familles à faire preuve de leadership, à créer et à résoudre des problèmes. Deux programmes sont offerts – [Technovation Girls](#) et [Technovation Families](#) – dans le cadre desquels enfants et adultes travaillent ensemble pour résoudre d'importants problèmes dans leur communauté. Il offre également des programmes en français.

Sites Web : <https://technovationchallenge.org/>, <http://technovationottawa.org/index.php/programme-francais/> et <https://www.technovationmontreal.com/>

Internet Safety for Kids & Families (en anglais) : Le programme Internet Safety for Kids and Families (ISKF) sensibilise les parents, les enseignants et les jeunes à la prévention et à la gestion des risques en ligne et soutient la citoyenneté numérique.

Site Web : https://www.trendmicro.com/en_my/initiative-education/internet-safety-kids-families.html

Le Centre Franco – Fiches d'activités sur l'identité et la citoyenneté numérique: Il s'agit de trois séries d'activités pédagogiques accompagnant les Modules de jeux-questionnaires iCN (identité et citoyenneté numérique) mis à la disposition des conseils scolaires. Ces activités sont prévues pour les élèves de la 3^e à la 10^e année, ainsi que pour les parents. La réalisation de ces activités ne requiert aucune technologie puisqu'elles misent sur les conversations, la communication orale et les échanges.

Site Web : <https://www.lecentrefranco.ca/tactic/ressources/fiches-dactivites-sur-lidentite-et-citoyennete-numerique/>

2.2 DE LA 7^E À LA 12^E ANNÉE (SECONDAIRES 1 À 5)

Girls Who Code : Les Clubs Girls Who Code sont des programmes éducatifs gratuits qui stimulent l'intérêt des filles de 11 à 18 ans pour la programmation et l'informatique. Les Clubs peuvent avoir lieu avant, pendant ou après l'école, la fin de semaine ou durant l'été. Dans les Clubs, les filles visionnent des tutoriels de programmation en ligne simples et amusants, renforcent leurs liens au moyen d'activités interactives, se familiarisent avec des modèles de femmes inspirants du secteur des technologies et collaborent pour résoudre des problèmes concrets au sein de leur collectivité. Certaines ressources sont bilingues.

Site Web : <https://frca.girlswhocode.com/>

Hackergal (en anglais) : Hackergal est un organisme de bienfaisance qui cherche à inspirer les filles d'un bout à l'autre du Canada à explorer les possibilités liées au codage. Comme les femmes sont fortement sous-représentées dans le domaine de la technologie, Hackergal déploie des efforts pour inspirer une nouvelle génération de programmeuses canadiennes et favoriser l'égalité des sexes dans cette industrie en plein essor.

Site Web : <https://hackergal.org/>

HabiloMédias : (le Centre canadien d'éducation aux médias et de littératie numérique) offre l'une des plus vastes collections de ressources dans ces domaines au monde – en anglais et en français. On y trouve des fiches-conseils, des infographies que les enseignants peuvent présenter à leurs élèves, et des jeux permettant d'initier les jeunes aux bonnes pratiques de cybersécurité. Les infographies et les ressources sont utiles pour aider les enseignants et les parents à favoriser l'adoption de bonnes pratiques de cybersécurité.

Site Web : <https://habilomedias.ca/>

Conseil des technologies de l'information et des communications (CTIC) – CyberTitan (en anglais) : L'Initiative canadienne d'éducation en matière de cybersécurité est mise en œuvre par le Conseil des technologies de l'information et des communications (CTIC) et est affiliée au programme CyberPatriot de l'Association des Forces aériennes des États-Unis présenté par la Fondation Northrop Grumman. La collaboration dans le cadre de ces programmes nationaux d'éducation en cybersécurité à l'intention des jeunes vise à promouvoir l'éducation et la sensibilisation dans le domaine de la technologie et l'excellence auprès des élèves des écoles intermédiaires et secondaires qui s'intéressent à une carrière en cybersécurité ou dans d'autres domaines de la science, de la technologie, de l'ingénierie et des mathématiques (STIM).

Site Web : <https://www.cybertitan.ca/>

Programme de concentration Focus sur les technologies de l'information (FTI) du CTIC : Le programme Focus sur les technologies de l'information (FTI) permet d'enseigner des compétences en technologies de l'information et des communications (TIC) aux élèves du secondaire. Il offre les éléments suivants :

- La concentration « médias interactifs » inclut la conception et le développement Web, les médias sociaux et mobiles, les jeux interactifs et le commerce électronique. Associez des compétences en gestion, en technologie et en leadership pour profiter de possibilités intéressantes au travail;
- La concentration « conception et développement de logiciels » inclut la conception, l'intégration, la programmation de solutions et le développement de base de données. Servez-vous de vos compétences techniques pour développer des applications et des systèmes qui permettront de résoudre des problèmes concrets;
- La concentration « analyse des systèmes de gestion et d'information » inclut l'analyse des systèmes de gestion et d'information ou de l'architecture des systèmes. Mettez à profit vos connaissances de la gestion et des affaires pour analyser les besoins en matière de gestion et proposer des solutions TIC permettant de combler les besoins de manière rentable;
- La concentration « systèmes de réseaux et leur exploitation » inclut la maintenance des plateformes techniques et de communication indispensables au bon fonctionnement d'une entreprise. Tirez parti de vos connaissances pour implanter le matériel et les logiciels vitaux et en assurer la maintenance;
- Les « compétences générales, et notamment les compétences en gestion et en technologie » aident les élèves à acquérir des connaissances en matière de leadership, de style de gestion et d'exploitation dans différentes entreprises. Grâce à leurs connaissances techniques, les élèves pourront accroître leur productivité en matière de TIC.

Site Web : <https://www.digitalyouth.ca/hub/fit/>

Fondation Raspberry Pi (en anglais) : La fondation Raspberry Pi a pour mission de mettre la puissance de l'informatique et du numérique dans les mains d'utilisateurs partout dans le monde. Son objectif est de permettre à un plus grand nombre de personnes d'exploiter cette puissance pour mieux travailler, résoudre les problèmes qu'ils tiennent à cœur et exprimer leur créativité.

Site Web : <https://www.futurelearn.com/partners/raspberry-pi>

CyberTaipan (en anglais) : CyberTaipan est une compétition australienne en cybersécurité qui s'inspire du programme [CyberPatriot](#) de l'Association des Forces aériennes des États-Unis. Ce programme a vu le jour il y a 11 ans et s'est établi au Canada sous le nom de [CyberTitan](#), au Royaume-Uni sous le nom de [CyberCenturion](#) et en Arabie Saoudite sous le nom de [CyberArabia](#). Dans le cadre de la compétition, des élèves du secondaire jouent le rôle de professionnels des TI nouvellement embauchés qui sont appelés à gérer le réseau d'une petite entreprise.

Site Web : <https://www.austcyber.com/educate/competitions-and-challenges/cybertaipan>

Projet CyberEdu : CyberEdu accompagne les enseignants dans la sécurité du numérique pour apporter les notions techniques, organisationnelles et de gouvernance de la sécurité du numérique. Le projet CyberEdu a vocation à intégrer la cybersécurité dans toutes les formations en informatique, qu'elles soient dispensées en écoles d'ingénieurs, universités ou écoles privées.

Site Web : <https://www.ssi.gouv.fr/actualite/cyberedu-des-documents-pedagogiques-a-destination-des-enseignants-en-informatique/>

Éduquer à la cybersécurité : La formation Éduquer à la cybersécurité permet aux enseignants de mieux comprendre l'importance de la cybersécurité, de s'initier aux moyens de se protéger en ligne, de disposer de pistes pour présenter ces nouvelles réalités aux élèves et ultimement de les intégrer dans la planification et le déroulement de leurs activités d'apprentissage. Pour en savoir plus sur cette formation, visitez cadre21.org. Cadre 21 accompagne les intervenants francophones du monde de l'éducation dans leur développement professionnel autour des grands enjeux de l'éducation au 21^e siècle.

Site Web : <https://cursus.edu/formations/43532/eduquer-a-la-cybersecurite>

Centre des éducateurs FTI : Le programme Focus sur les technologies de l'information (FTI) permet d'enseigner des compétences en technologies de l'information et des communications (TIC) aux élèves du secondaire. Il a pour but d'inciter les jeunes Canadiens à poursuivre des études postsecondaires et à entrer sur le marché du travail en possédant les compétences numériques et en TIC recherchées qui les aideront à atteindre leurs objectifs professionnels.

Site Web : <https://www.jeunessenumerique.ca/centre-des-educateurs/tif/>

Journées d'apprentissage pour les élèves de Jeunesse numérique : Les journées d'apprentissage permettent aux élèves de niveau intermédiaire et secondaire d'acquérir les compétences numériques dont ils auront besoin pour leur future vie professionnelle. Les élèves participent à une demi-journée ou à une journée complète d'activités

d'apprentissage par l'expérience qui sont axées sur des thèmes liés aux technologies de l'information et des communications, comme la cybersécurité et la cybercitoyenneté.

Site Web : <https://www.jeunessenumerique.ca/programmes/>

Enfants Avertis : Enfants avertis est le programme national interactif d'éducation à la sécurité du Centre canadien de protection de l'enfance (CCPE) conçu pour les enfants de la maternelle à la 9^e année (3^e secondaire). Il aide les enseignants à apprendre aux enfants et aux adolescents des stratégies de sécurité personnelle efficaces au moyen d'activités amusantes, interactives et adaptées à l'âge des élèves, de manière à développer leur résilience et à réduire leur vulnérabilité autant sur Internet que dans la vraie vie.

Site Web : <https://www.kidsintheknow.ca/app/fr/about>

CyberJulie : CyberJulie fait partie du programme Enfants avertis, qui apprend aux enfants à mieux se protéger.

Site Web : <http://cyberjulie.ca/app/fr/>

Canada en programmation: Canada en programmation conçoit et met en œuvre des programmes d'apprentissage de la technologie et établit des partenariats d'enseignement pour toute la population du Canada.

Site Web : <https://www.canadalearningcode.ca/fr/accueil/>

Programme de formation pour les enseignants des STIM : Ce programme de formation dans les compétences STIM est offert aux enseignants de la maternelle à la 12^e année. Axé sur le perfectionnement professionnel, il est conçu pour les aider à mieux outiller les jeunes et ainsi les rehausser.

Site Web : <https://www.actua.ca/fr/>

3 RESSOURCES POSTSECONDAIRES

National Security Collaboration Center (en anglais) : Cette initiative vise à créer le National Security Collaboration Center (NSCC) au sein de la University of Texas at San Antonio (UTSA) pour faire avancer la recherche, l'éducation et le perfectionnement professionnel dans les domaines de la cybersécurité, de l'analytique des données et de l'infonuagique. Le NSCC permettra de créer un écosystème collaboratif efficace dans le cadre duquel le gouvernement, l'industrie et le milieu universitaire travailleront ensemble pour régler les grands enjeux nationaux liés à la cybersécurité.

Site Web : <http://www.utsa.edu/president/reporting-offices/nscc/>

Guide de Springboard sur les salaires en cybersécurité (en anglais) : Ce guide complète bien la [feuille de route sur la certification](#) de CompTIA et sert de référence utile à ceux et celles qui souhaitent se lancer dans le domaine. Il donne un aperçu des carrières dans le secteur de la cybersécurité et des renseignements détaillés sur les salaires connexes, selon le rôle, le lieu de travail et le niveau de scolarité ou de certification.

Site Web : <https://www.comptia.org/content/it-careers-path-roadmap>

Glossaire de termes liés à la cybersécurité de Cybrary (en anglais) : Le monde des TI comporte tout un jargon, et la terminologie peut prêter à confusion. Le glossaire exhaustif de termes anglais de Cybrary constitue une excellente ressource pour mieux s'y retrouver. Il définit des termes généraux de cybersécurité que le grand public risque de connaître (comme l'hameçonnage ou le cheval de Troie [« [Trojan Horse](#) »]), de même que des notions plus complexes s'adressant aux professionnels des TI, comme le programme WHOIS et le terme « [TCP full open scan](#) ».

Site Web : <https://www.cybrary.it/glossary/>

Cybersecurity Education for Universities (en anglais) : Dans le cadre de son programme Cybersecurity Education for Universities (CEU) créé pour combler certaines lacunes dans les programmes postsecondaires en cybersécurité, TrendMicro offre gratuitement des conseils, de l'expertise et du soutien en la matière. Il travaille en collaboration avec les établissements universitaires et privilégie généralement l'un ou plusieurs des domaines suivants :

- Encadrement et formation du corps professoral;
- Harmonisation avec le curriculum et consultation sur les cours;
- Séminaires et webinaires techniques.

Site Web : https://www.trendmicro.com/en_my/initiative-education/cybersecurity-education-universities.html

Center for Cyber Safety and Education (en anglais) : Le Center for Cyber Safety and Education est la fondation de bienfaisance sans but lucratif d'(ISC)², un organisme qui favorise l'éducation et accorde des certifications dans le domaine de la cybersécurité. Il offre des programmes d'éducation et de sensibilisation à l'intention des élèves, des parents, des enseignants et des membres du public de tous les âges et de tous les horizons pour les aider à mener leurs activités en ligne en toute sécurité.

Site Web : <https://iamcybersafe.org/s/>

Cours « Foundations of Cybersecurity » de Springboard (en anglais) : Que vous veniez de commencer votre carrière dans le domaine de la cybersécurité ou que vous souhaitiez revoir vos connaissances de base, le cours « Foundations of Cybersecurity » de Springboard constitue le point de départ idéal. Dans le cadre de ce cours gratuit comportant 38 heures de contenu et 40 ressources réparties parmi neuf modules, vous vous familiariserez avec les fondements nécessaires pour approfondir vos connaissances dans le domaine. Il suffit de cliquer sur le lien pour prendre connaissance du programme et lancer le cours.

Site Web : <https://www.springboard.com/resources/learning-paths/cybersecurity-foundations/>

Formation et ressources gratuites de Cybrary (en anglais) : Que votre expérience de la sécurité de l'information corresponde au niveau débutant, intermédiaire ou expert, Cybrary saura vous offrir de la formation et des cours adaptés à vos compétences. Le catalogue compte plus de 150 cours, y compris des séances de formation sur la cryptographie, la programmation sécurisée, les techniques avancées de tests d'intrusion, la gestion de la virtualisation, et plus encore.

Site Web : <https://www.cybrary.it/catalog/cybersecurity/>

Cours « Cyber Aces Online » de SANS (en anglais) : Le SANS Institute a élaboré ce cours gratuit dans le but de pallier le manque de professionnels de la cybersécurité en initiant des étudiants et des professionnels d'autres milieux au domaine. Le cours vise à enseigner aux débutants un grand nombre des principes de base nécessaires pour lancer sa carrière en cybersécurité.

Site Web : <https://www.cyberaces.org/>

Cyber Security Education (en anglais) : CybersecurityEducation.org constitue un répertoire en ligne de programmes d'études et de carrières en cybersécurité. Le répertoire se veut une ressource de choix qui offre de nombreuses options aux étudiants :

- Trouver des établissements d'enseignement par lieu, diplôme ou sujet;
- Comparer les établissements et faire de la recherche sur ceux-ci;
- Demander de l'information gratuite auprès des établissements;
- Explorer les options sur le plan de l'éducation et les débouchés.

Site Web : <https://www.cybersecurityeducation.org/resources/>

Cyber Nouveau-Brunswick (CyberNB) : CyberNB intervient sur quatre grands axes pour développer un écosystème de cybersécurité intégré, reconnu sur la scène internationale, couvrant l'éducation, les carrières professionnelles, la recherche, la commercialisation, etc. Cette organisation bilingue offre de nombreuses ressources aux enseignants et aux élèves pour les aider à améliorer leurs connaissances et leurs compétences en cybersécurité.

Site Web : <https://cybernb.ca/Accueil.htm>

4 RESSOURCES GOUVERNEMENTALES

4.1 RESSOURCES DU GOUVERNEMENT DU CANADA

Carrefour de l'apprentissage : Le Carrefour de l'apprentissage est un réputé prestataire d'activités et de programmes d'apprentissage s'adressant aux professionnels de la cybersécurité et de la [COMSEC](#) qui travaillent au gouvernement du Canada ou chez nos partenaires nationaux. Il propose également des services, de l'orientation et des conseils en matière de formation en cybersécurité aux intervenants de l'industrie, du milieu universitaire et des autres ordres de gouvernement. Il s'agit d'une ressource bilingue.

Site Web : <https://cyber.gc.ca/fr/carrefour-de-lapprentissage>

Pensez cybersécurité : Pensez cybersécurité est une campagne nationale de sensibilisation publique conçue pour sensibiliser les Canadiens à la sécurité en ligne et les informer des étapes à suivre pour se protéger en ligne. Cette campagne est menée par le Centre pour la cybersécurité et vise à fournir des conseils et de l'orientation au grand public et aux personnes qui souhaitent s'initier à la cybersécurité. Il s'agit d'une ressource bilingue.

Site Web : <https://www.pensezcybersecurite.gc.ca/fr/homepage>

Emploi et Développement social Canada : Programmes et politiques en matière d'emploi et de développement social et activités liées à leur élaboration qui visent à appuyer le gouvernement du Canada. Cela comprend des consultations, des cadres, des plans et des recherches. Il s'agit d'une ressource bilingue.

Site Web : <https://www.canada.ca/fr/emploi-developpement-social/programmes.html>

Gendarmerie royale du Canada (GRC) : L'une des priorités stratégiques de la GRC consiste à réduire l'activité des jeunes dans la criminalité et leur présence parmi les victimes. Il s'agit d'une ressource bilingue.

Sites Web : <https://www.rcmp-grc.gc.ca/cycp-cpcj/is-si/isres-ressi-fra.htm> et <https://www.rcmp-grc.gc.ca/fr/securite-des-jeunes/centre-de-prevention-du-crime-chez-les-jeunes>

4.2 RESSOURCES DE PAYS ALLIÉS DU CANADA

Département de la Sécurité intérieure des États-Unis (en anglais) : Le Département de la Sécurité intérieure déploie des efforts pour protéger les États-Unis contre les nombreuses menaces qui pèsent sur le pays. Pour ce faire, il compte sur le dévouement de plus de 240 000 employés travaillant dans toute une gamme de domaines, qu'il s'agisse de l'aviation, de la sécurité frontalière ou de l'intervention en cas d'urgence, en passant par les analystes en cybersécurité et les inspecteurs d'installations chimiques.

Site Web : <https://www.dhs.gov/be-cyber-smart/cyber-lessons#section-app-security>

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (en anglais) : Le National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), publié par le National Institute of Standards and Technology (NIST) dans la [NIST Special Publication 800-181](#), est une ressource nationale qui vise à établir la taxonomie et un lexique commun des termes liés au travail et aux travailleurs dans le domaine de la cybersécurité, quel que soit le lieu de travail et l'employeur.

Sites Web : <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center> et <https://studentprivacy.ed.gov/topic/security-best-practices>

National Integrated Cyber Education Research Center (NICERC) (en anglais) : Des spécialistes des programmes d'études du NICERC se rendent aux quatre coins du pays pour donner des ateliers de perfectionnement professionnel aux enseignants de la maternelle à la 12^e année. Ces ateliers donnent aux enseignants l'information et les ressources dont ils ont besoin pour enseigner le programme à leurs élèves, sensibiliser ceux-ci aux enjeux liés à la cybersécurité et les encourager à faire carrière dans le domaine.

Site Web : <https://www.dhs.gov/be-cyber-smart/cyber-lessons#section-app-security>

The National Cyber Security Centre (NCSC) (en anglais) : Le NCSC se veut un point de contact central pour les spécialistes, les grandes organisations, les organismes gouvernementaux, le public et les ministères. Il travaille également en collaboration avec d'autres organismes d'application de la loi, des organisations chargées de la défense, les organismes de renseignement et de sécurité du Royaume-Uni et des partenaires internationaux. Les infographies qui se trouvent sur cette page s'adressent autant aux étudiants d'établissements postsecondaires qu'aux élèves des cycles primaires, intermédiaires et secondaires. Elles permettent également d'orienter les enseignants qui souhaitent créer leurs propres outils pédagogiques sur la cybersécurité.

Sites Web : <https://www.ncsc.gov.uk/information/resources-for-schools> et https://www.ncsc.gov.uk/files/NCSC_NEN-cards-english-home-print.pdf

AustCyber (en anglais) : AustCyber vise à créer un écosystème de cybersécurité en Australie, à exporter la cybersécurité australienne à l'échelle internationale et à faire de l'Australie un chef de file de l'éducation en cybersécurité.

Site Web : <https://www.austcyber.com/>

CySCA (en anglais) : CySCA est une compétition de « piratage » organisée par un regroupement d'organismes gouvernementaux, d'entreprises et de professionnels du milieu universitaire de l'Australie qui cherchent à découvrir la prochaine génération de talents australiens en cybersécurité.

Site Web : <https://www.cyberchallenge.com.au/>

Formation virtuelle du Département de la Sécurité intérieure des États-Unis (en anglais) : Ce site offre des cours et du matériel de formation gratuits à quiconque souhaite mieux connaître la sécurité des systèmes de contrôle industriels. On y trouve 11 cours sur toute une gamme de sujets, notamment la sécurité opérationnelle pour les systèmes de contrôle et les tendances actuelles des vulnérabilités liées à la cybersécurité qui posent un risque pour les systèmes de contrôle industriels. Si vous préférez suivre des cours en personne, l'organisme offre également des cours donnés par des instructeurs.

Site Web : <https://ics-cert-training.inl.gov/learn>

Programme Safe Online Surfing (SOS) du FBI (en anglais) : Le programme éducatif gratuit FBI-SOS vise à promouvoir la citoyenneté numérique en permettant aux élèves de la 3^e à la 8^e année d'apprendre les fondements de la sécurité en ligne tout en s'amusant. Le site établit pour les enseignants un curriculum conforme aux exigences fédérales et à celles des états en matière de sécurité sur Internet, en plus d'offrir des tests en ligne et une compétition nationale visant à favoriser l'apprentissage et la participation des élèves.

Site Web : <https://www.fbi.gov/fbi-kids>

5 RESSOURCES SUPPLÉMENTAIRES

5.1 BLOGUES

Billets de blogue de Springboard sur la cybersécurité (en anglais) : Le blogue vise à expliquer toute une gamme de sujets liés à la cybersécurité et à présenter de l'information gratuite pour aider les professionnels à faire avancer leur carrière ou à [percer dans le domaine](#). Qu'il s'agisse de recommandations sur les [langages de programmation](#) à apprendre ou de conseils sur la [rédaction d'un curriculum vitae pour des postes en cybersécurité](#), de nouveaux billets sont publiés fréquemment sur le blogue pour tenir les lecteurs au courant.

Site Web : <https://www.springboard.com/blog/category/cybersecurity/>

Schneier on Security (en anglais) : Le blogue Schneier on Security se classe systématiquement parmi les meilleurs sites Web personnels portant sur la cybersécurité dans la blogosphère, et pour cause. Son auteur, l'expert en sécurité Bruce Schneier, est [reconnu dans le domaine](#). En plus d'occuper le poste de dirigeant principal de la technologie chez IBM Resilient, il est chercheur universitaire au Berkman Center de l'Université Harvard et un collaborateur fréquent [dans les médias](#).

Site Web : <https://www.schneier.com/>

Krebs on Security (en anglais) : Le blogue de Brian Krebs est lui aussi très reconnu dans le domaine de la cybersécurité. M. Krebs a travaillé comme journaliste au Washington Post de 1995 à 2009 et a rédigé plus de 1 300 billets pour le blogue Security Fix. Il s'est intéressé davantage au sujet lorsqu'une attaque a ciblé son réseau à domicile en 2001. Son blogue influent concerne souvent des enquêtes sur des crimes en ligne, des violations de données et la cyberjustice.

Site Web : <https://krebsonsecurity.com/>

5.2 VIDÉOS ET WEBINAIRES

Conférences TED sur la cybersécurité (en anglais) : Les conférences TED sont reconnues pour leur style captivant, leur nature informative et leur limite de 18 minutes. Leur visionnement est également gratuit. Des douzaines de conférences TED et TEDx sur la cybersécurité se trouvent sur des plateformes comme YouTube et le [site Web TED](#). Ce [billet de blogue de Springboard](#) présente 12 conférences TED et TEDx fascinantes autant pour les professionnels que pour ceux qui s'intéressent tout simplement à la cybersécurité.

Site Web : <https://www.springboard.com/blog/12-must-watch-cybersecurity-ted-talks/>

Webinaires et vidéos gratuits de l'Université Stanford portant sur la cybersécurité (en anglais) : Stanford offre gratuitement des [webinaires sur la cybersécurité](#) et une série de conférences en ligne mettant en vedette ses spécialistes de la cybersécurité. L'université présente également des vidéos gratuites sur l'informatique et la sécurité sur sa [chaîne YouTube](#).

Site Web : <https://computersecurity.stanford.edu/free-online-videos>

Flux de webinaires BrightTALK : BrightTALK offre un flux exhaustif de webinaires liés à la cybersécurité donnés par des experts et des leaders éclairés. Des milliers de vidéos sont accessibles sur le flux consacré à la sécurité des TI, qui est mis à jour en continu. Les webinaires de BrightTALK intéresseront particulièrement les professionnels dont la carrière en cybersécurité est bien entamée, et des options s'offrent dans plusieurs langues.

Site Web : <https://www.brighttalk.com/community/it-security>

Webinaires BeyondTrust : Le fournisseur de solutions de cybersécurité BeyondTrust offre toute une gamme de produits qui permettent aux entreprises de se protéger contre les cybermenaces, en plus d'une série de ressources éducatives comme des webinaires, des livres blancs, des fiches techniques et des études de cas. Ses webinaires portent sur les pratiques exemplaires, des conseils d'experts sur la façon de combler les lacunes de sécurité et d'autres notions connexes pour aider les organisations à se défendre contre les attaques.

Site Web : <https://www.beyondtrust.com/fr/resources/webcasts#cardLang=fr>

Introduction aux carrières en cybersécurité du InfoSec Institute (en anglais) : Cette vidéo s'adresse aux élèves de la maternelle à la 12^e année et explique la pénurie de compétences en cybersécurité tout en les encourageant à faire carrière dans ce domaine en plein essor. Elle affronte les préjugés et les stéréotypes associés à l'industrie en définissant ce que font les professionnels en cybersécurité et la vaste gamme de rôles qu'ils peuvent être appelés à jouer. La vidéo présente également des conseils sur les mesures que peuvent prendre les élèves pour se préparer à une carrière dans le domaine, notamment suivre des cours en ligne, trouver un mentor et participer à des compétitions comme les Global Cyber Olympics.

Site Web : <https://www.youtube.com/watch?v=-AkuKKJ8dN0>

branchÉ : Trois vidéos de *branchÉ* sont disponibles sur la chaîne YouTube. *branchÉ* était une ressource en ligne gratuite portant sur la sécurité sur Internet et conçue pour les élèves de 4^e, 5^e et 6^e année. Elle avait comme objectif d'aider les élèves à développer des comportements en ligne sains et sûrs, tels que la netiquette, la sécurité, la protection des renseignements personnels, et les relations personnelles (par exemple, reconnaître et gérer la cyberintimidation), de la même façon dont ils le feraient dans la vie de tous les jours. Malheureusement, la ressource complète n'est plus disponible.

Site Web : https://www.youtube.com/playlist?list=PL-3fUblIRJtJULV8_MZR4a1A7qHvq0Vuu

5.3 BALADOS

Risky Business (en anglais) : Ce balado offre du contenu lié à la cybersécurité accessible en tout temps. Lancé en 2007, Risky Business se démarque par l'attention qu'il accorde aux nouvelles de l'industrie et par ses entrevues avec des invités intéressants.

Site Web : <https://risky.biz/about/>

Security Weekly (en anglais) : Security Weekly, l'un des premiers balados sur la cybersécurité, s'adresse à la collectivité de la sécurité de l'information depuis 2005. Les balados sont accompagnés de notes détaillées et sont [diffusés en direct](#) sur YouTube et Facebook.

Site Web : <https://securityweekly.com/>

Security Now (en anglais) : Accessible en format audio et vidéo, Security Now est un balado hebdomadaire animé par Leo Laporte, fondateur de TWiT Netcast Network, et Steve Gibson, qui a créé le premier programme antiespiogiciel (et à qui on attribue la création du terme *spyware*). L'émission dure environ deux heures et vise à aider les auditeurs à renforcer leur sécurité personnelle en abordant divers sujets comme la sécurité des mots de passe, les pare-feux et les réseaux privés virtuels.

Site Web : <https://twit.tv/shows/security-now>

StormCast du Internet Storm Center (en anglais) : Si un balado de deux heures vous semble trop long, tournez-vous plutôt vers les mises à jour quotidiennes rapides de SANS Internet Storm Center. Ces « StormCasts » résument les actualités liées à la sécurité réseau en plus ou moins cinq minutes, un choix idéal pour se divertir pendant l'aller-retour au travail.

Site Web : <https://isc.sans.edu/podcast.html>

Exploring Information Security (en anglais) : L'animateur Timothy De Block a commencé sa carrière en informatique comme technicien en électronique dans les Forces navales des États-Unis. Après avoir quitté le milieu militaire, il s'est découvert un intérêt pour la sécurité et a fini par décrocher un poste d'agent de la sécurité de l'information au sein d'une agence d'État en Caroline du Sud. Chaque semaine, il partage son expertise et discute des actualités et des nouvelles tendances avec des leaders de l'industrie de l'INFOSEC.

Site Web : <http://www.timothydeblock.com/eis>

La French Connection : Ce balado international porte sur la sécurité et le piratage et présente des nouvelles et des opinions du Québec et de l'Europe.

Site Web : <https://securite.fm/>

France culture : Balados, émissions et articles faisant la lumière sur la cybersécurité.

Site Web : <https://www.franceculture.fr/theme/cybersecurite>

5.4 JEUX EN LIGNE

Interland : Be Internet Awesome apprend aux enfants les fondements de la citoyenneté numérique et de la sécurité pour qu'ils puissent explorer le monde virtuel avec confiance.

Site Web : https://beinternetawesome.withgoogle.com/fr_all/interland

Cybersafe Care (en anglais) : Cybersafe Care est une campagne d'éducation publique visant à aider les parents, les gardiens et les éducateurs à assurer la sécurité des enfants en ligne et à guider ceux-ci dans l'utilisation sécuritaire de la technologie et des médias sociaux. Il s'agit d'une source d'information fiable (qui donne des renseignements propres à l'Île-du-Prince-Édouard) qui permettra à tous ceux qui s'occupent des enfants de veiller à ce que les jeunes possèdent les connaissances nécessaires pour naviguer en ligne en toute sécurité.

Site Web : <https://www.cybersafecarepei.ca/>