Sécurise ton réseau

5e à la 7e année

Actua | 111 Murray Street, Ottawa, ON K1N 5M5 | www.actua.ca | 613 234 4137

Jeunesse · STIM · Innovation
Youth · STEM · Innovation

Sécurise ton réseau

Conditions d'utilisation

Avant de réaliser cette activité en tout ou en partie, vous reconnaissez et acceptez ce qui suit :

- il vous appartient de passer en revue toutes les sections du présent document et la documentation connexe ainsi que d'appliquer les consignes de sécurité nécessaires à la protection de toutes les personnes concernées;
- les mesures précisées à la rubrique « Consignes de sécurité » du présent document ne sont pas exhaustives ni ne remplacent votre propre cadre d'examen de la sécurité;
- Actua n'est pas responsable des dommages attribuables à l'usage du présent contenu;
- Vous pouvez adapter ce document à vos besoins (le remanier, le transformer ou créer du matériel à partir de celui-ci), à condition d'indiquer qu'Actua en est l'auteur original et que vous y avez apporté des changements. Ce contenu ne peut être transmis à de tierces parties sans la permission écrite d'Actua.

À propos d'Actua

Représentant plus de 40 universités et collègues à travers le pays, Actua est le principal réseau de sensibilisation des jeunes aux sciences, à la technologie, à l'ingénierie et aux mathématiques (STIM) au Canada. Chaque année, 350 000 jeunes prennent part à des ateliers pratiques, à des camps et à des projets communautaires inspirants dans plus de 500 localités d'un océan à l'autre. Actua met l'accent sur la participation de jeunes sous-représentés dans le cadre de programmes destinés aux Autochtones, aux filles et aux jeunes femmes, aux jeunes à risque ainsi qu'à ceux vivant dans des communautés nordiques ou éloignées. Pour de plus amples renseignements, consultez notre site web à actua.ca et suivez-nous sur Twitter, Facebook, Instagram et YouTube!

Sécurise ton réseau

Présentation de l'activité

Dans cette activité, les élèves découvriront les diverses arnaques en ligne et hors ligne dont se servent les cybercriminels pour tenter de s'emparer des renseignements personnels d'utilisateurs trop confiants. Après avoir appris les différentes façons dont les arnaqueurs utilisent les pièges à clics et l'hameçonnage, les jeunes mettront en pratique leurs nouvelles connaissances pour jouer aux cyberdétectives. Grâce à cette activité, elles et ils sauront employer des stratégies proactives pour contrer diverses cybermenaces.

Cette activité fait partie d'une série d'activités basées sur l'éducation cybernétique. La suite comprend : La citoyenneté numérique et toi, La présence en ligne, Cyberdétective, La nétiquette, Craque le code et Sécurise ton réseau. Explorez le Guide pédagogique pour former des jeunes cyberfutés pour apprendre comment vous pouvez introduire l'éducation cybernétique dans votre milieu éducatif.

Activité conçue par Actua, 2022.

Environnement	Durée	Public cible	Spécifications techniques
En personne	1 heure	5e-7e année (10-13 ans)	Certains exercices nécessitent l'utilisation d'un ordinateur portable ou d'une tablette. Moyennant certaines modifications, on peut regrouper les élèves en équipes de deux ou plus. **Les responsables de l'animation doivent avoir à leur disposition un ordinateur portable, un projecteur, des haut-parleurs et un écran ou un mur vierge pour y faire des projections.**

Environnement	Durée	Public cible	Spécifications techniques
			• Projecteur • Haut-parleurs • Écran ou mur vierge • Ordinateurs portables ou tablettes

Résultats d'apprentissage

À la fin de l'activité, les élèves connaîtront :

- les diverses formes de cyberarnaques et de tentatives d'hameçonnage ainsi que les façons d'éviter celles-ci;
- les mesures préventives servant à contrer les cybermenaces;
- les meilleures pratiques pour naviguer et communiquer en ligne de manière réfléchie et proactive.

OUTILS	COMPÉTENCES	ATTITUDES
Connaissances, ressources et expériences • Piège à clics • Hameçonnage • Confidentialité • Renseignements personnels	**Compétences numériques et en STIM, et aptitudes essentielles à l'employabilité et à la vie quotidienne** • Littératie numérique • Utilisation des appareils • Comportement sûr et responsable en ligne	**Intelligence numérique, action communautaire et pensée computationnelle** • Compréhension de sa relation avec la technologie • Gestion des renseignements personnels

OUTILS	COMPÉTENCES	ATTITUDES
	• Communication en ligne • Jugement critique • Faculté d'analyse	

Logistique (durée, taille du groupe, matériel)

Section	Durée	Taille du groupe	Matériel
Introduction	10 min	*Tout le groupe*	**Responsable de l'animation** • Image d'un piège à clics (voir l'annexe C)
1. Les cyberarnaques	20 min	*Individuellement; tout le groupe*	**Responsable de l'animation** • Stay Safe from Phishing and Scams (sous-titres en français) • Les cyberarnaques : hameçonnage et piège à clics (présentation) **Par élève** • Ordinateur portable ou tablette • Questionnaire sur l'hameçonnage
2. Les pratiques cybersécuri-taires	20 min	*Individuelle-ment; tout le groupe*	**Responsable de l'animation** • 5 Tips for Cybersecurity Safety brought to you by Mayim Bialik (sous-titres en français) **Par élève** • Papier et crayon • Ordinateur portable ou tablette

Section	Durée	Taille du groupe	Matériel
			• Interland de Google (La rivière de la réalité)
Réflexion et récapitulation	10 min	*Tout le groupe; individuelle-ment*	**Par élève** • Ordinateur portable ou tablette • Outil de création d'affiches Canva

Consignes de sécurité

Les consignes de sécurité ci-dessous ne sont pas exhaustives. Veillez à passer en revue l'activité et à inspecter l'environnement où elle sera réalisée afin de déterminer si des mesures additionnelles sont requises pour assurer la sécurité des élèves.

Sécurité émotionnelle

Ce projet vise à fournir aux jeunes les outils et les connaissances nécessaires pour comprendre les comportements en ligne et prendre des décisions sécuritaires.

- Tenez compte du fait que les élèves n'ont pas toutes et tous les mêmes expériences et connaissances en matière de pratiques cybersécuritaires, de cybersécurité et de citoyenneté numérique. La présente activité pourrait vous amener à discuter de sujets délicats, comme la cyberintimidation et d'autres cyberrisques. Veuillez préserver en tout temps la sécurité émotionnelle des jeunes et vous reporter à la formation reçue à votre établissement et pour ce projet.
- Orientez la discussion vers les comportements sains et sûrs en ligne et encouragez les jeunes à faire des choix responsables, informés et judicieux.

Sécurité en ligne

Certains volets de cette activité nécessitent l'usage d'appareils connectés à Internet.

- Examinez au préalable les vidéos, les sites web et le matériel prévus afin de vous assurer qu'ils conviennent à vos élèves.

- Au besoin, rappelez aux jeunes de se concentrer sur la tâche à faire et d'utiliser uniquement les liens fournis pour l'activité.
- Donnez l'exemple et encouragez l'adoption de comportements appropriés en ligne (poser des questions et y répondre dans la boîte de clavardage, employer un langage positif et motivant, utiliser les appareils uniquement pour réaliser l'activité, etc.).

Liens avec le programme d'études

Chacune des activités s'aligne avec ces trois aspects du Cadre de référence pancanadien pour l'enseignement de l'informatique :

Ordinateurs et réseaux : Cybersécurité

- L'élève débutant devrait pouvoir définir le concept de cybersécurité et créer des mots de passe sûrs selon des critères d'efficacité. L'élève compétent devrait pouvoir décrire des types courants de cyberattaques et reconnaître le contenu malveillant, appliquer des moyens de prévention et évaluer le rôle joué par les personnes dans la création, la prévention et la réduction de la portée des cyberattaques ainsi que leurs effets sur la population et la société (p. 24).

Données : Gouvernance des données

- L'élève débutant devrait pouvoir nommer des manières dont les activités numériques ou physiques créent des données numériques et régler les paramètres de confidentialité sur des outils numériques couramment utilisés. L'élève compétent devrait pouvoir déterminer qui possède ses données numériques, évaluer les lois et les politiques provinciales et fédérales sur la gouvernance des données et les accords autochtones sur la gouvernance des données et comprendre, ainsi que défendre ses droits par rapport aux données et ceux des autres (p. 26).

Technologie et société : Éthique, sécurité et politique

- L'élève débutant devrait pouvoir décrire des stratégies pour protéger ses renseignements personnels et son identité en ligne. L'élève compétent devrait pouvoir définir et appliquer des principes de base en lien avec les droits d'auteur, expliquer les problèmes liés à la vie privée et évaluer les effets de la cybercriminalité et du piratage sur soi-même et la société (p. 28).

Marche à suivre

Préparation

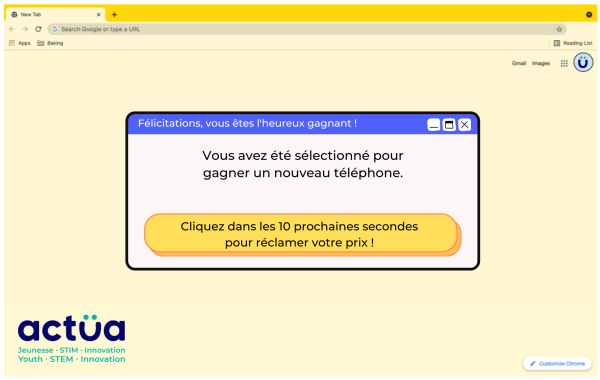
Section	Préparation

Généralités	• **Préparez l'activité et les mesures d'adaptation requises, s'il y a lieu :**
	  ○ Déterminez votre **mode d'enseignement** et puisez des idées, au besoin, dans les sections Recommandations selon le mode d'enseignement et Possibilités d'adaptation.
	  ○ Même si la **durée estimée** est précisée, il peut être utile de réfléchir au temps que vous voulez consacrer aux différents exercices et aux discussions.
	  ○ La **taille du groupe** indiquée (en équipes de deux ou plus, ou individuellement) n'est qu'une suggestion et peut être adaptée aux besoins de votre classe.
	• **Contenu :**
	  ○ Préparez des **réponses** aux diverses questions de réflexion posées durant l'activité.
	  ○ Examinez les vidéos et le matériel fournis à l'annexe C pour déterminer si leur contenu **convient** à vos élèves.
	• **Matériel :**

Section	Préparation
	○ Vérifiez que votre appareil, l'écran et le projecteur sont bien installés et fonctionnels. ○ Préparez les appareils des élèves.
Introduction	• Préparez l'image à afficher ou à projeter.
1. Les cyberarnaques	• Prenez connaissance du Questionnaire sur l'hameçonnage.
2. Les pratiques cybersécuritaires	• Familiarisez-vous avec le jeu Interland de Google (La rivière de la réalité) (Remarque : Le jeu comporte du son, mais il s'agit seulement d'une voix hors champ qui lit les mots apparaissant à l'écran. Il n'est pas nécessaire d'avoir du son pour jouer).
Réflexion et récapitulation	• Explorez la plateforme Canva (Remarque : aucun compte requis pour l'utiliser).

Introduction

1. Affichez ou projetez cette image ci-contre afin que les élèves la remarquent en entrant dans la classe.
2. Présentez le scénario : « Vous naviguez sur Internet avant le début de la classe, quand soudainement ce message surgit sur votre écran. Apparemment, vous courez la chance de gagner un nouveau téléphone! **Qu'en pensez-vous? Devriez-vous faire tourner la roue?** »



3. Dévoilez la vérité : « Il s'agit d'un exemple d'une arnaque très courante sur Internet (le piège à clics) que nous allons examiner en détail plus loin. » (Pour en savoir plus, voir l'annexe B, Information documentaire.)
4. Naviguer en ligne, ça peut être amusant et éducatif si on sait repérer les pièges. Démarrez un remue-méninges en posant la question suivante : **« Quels risques nous guettent sur Internet? »**.
    a. *Réponses possibles :* *Pièges à clics, cyberintimidation, tentatives d'hameçonnage, vols de renseignements personnels, se faire escroquer par une personne inconnue.*
5. Réorientez la discussion vers les pratiques cybersécuritaires en posant cette question : **« Connaissez-vous des stratégies pour vous protéger contre ces risques ? ».**

1. Les cyberarnaques

La photo présentée en introduction constitue un exemple de cyberarnaque courante : le piège à clics. Explorez celui-ci et une autre forme répandue de cyberarnaque : l'hameçonnage.

1. Montrez cette vidéo, Stay Safe from Phishing and Scams (Google for Education, 3:14, sous-titres en français), qui présente les cyberarnaques et les principales stratégies pour les éviter.
2. Présentez le contenu de Les cyberarnaques : hameçonnage et piège à clics.
    a. Pour chaque exemple, demandez aux élèves s'il s'agit d'une cyberarnaque et, si oui, d'indiquer les signaux d'alarme.
    b. Les *Notes du présentateur* indiquent les éléments à faire remarquer aux élèves dans chaque exemple.
3. Invitez les élèves à remplir le Questionnaire sur l'hameçonnage (individuellement ou en équipes de deux ou plus).
    a. **Remarque :** nom d'utilisateur : cyberfuté; courriel : cyberfute@gmail.com.
4. Demandez aux jeunes ce que cet exercice leur a appris à propos des stratégies à appliquer pour protéger leur boîte de réception (ou ce qu'elles et ils ont appris ailleurs à ce sujet).

    a. Réponses possibles : Avant de cliquer sur un lien, le survoler avec la souris afin de révéler l'adresse URL; examiner l'adresse courriel de l'expéditeur pour repérer tout élément suspect; vérifier si le courriel contient des fautes d'orthographe et de grammaire, etc.

5. Présentez les étapes à suivre en cas de **divulgation accidentelle de renseignements personnels ou sensibles :**
    a. Contacter la plateforme concernée (p. ex. s'il s'agit de renseignements bancaires, contacter l'institution financière);
    b. Contacter les autorités policières locales;
    c. Contacter le Centre antifraude du Canada.

2. Les pratiques cybersécuritaires

1. Montrez cette vidéo : 5 Tips for Cybersecurity Safety brought to you by Mayim Bialik (IBMorg, 5:45, sous titres en français).
    a. **Remarque :** Les élèves peuvent noter par écrit les trucs qu'elles et ils ignoraient.
2. **« Parmi les stratégies que vous avez apprises (dans la vidéo ou ailleurs), lesquelles peuvent vous aider à devenir une utilisatrice ou un utilisateur numérique responsable? »**
    a. Amorces : cyberarnaques; sécuriser son réseau; partage d'informations.
    b. Réponses possibles : Protéger la confidentialité de ses profils et de ses comptes, éviter de divulguer ses renseignements personnels, accepter dans son réseau uniquement les personnes qu'on connaît, créer des mots de passe forts et uniques pour tous ses comptes, ne pas croire tout ce qu'on lit en ligne, ne pas cliquer sur n'importe quoi, etc.
3. Invitez les élèves à jouer à Interland de Google (La rivière de la réalité) pendant 10 minutes. Il y a d'autres jeux sur la plateforme, mais concentrez-vous sur La rivière de la réalité.
    a. Demandez aux élèves de noter leurs bonnes réponses, en particulier celles qui leur ont permis d'apprendre de nouvelles stratégies.
    b. ***Remarque :*** Le jeu peut être lent selon le type d'appareil et de connexion Internet dont les élèves disposent. En cas de lenteur, on peut

désactiver la résolution HD en cliquant sur l'icône d'engrenage dans le coin inférieur droit. Toutefois, la modification de ce paramètre oblige les élèves à recommencer le jeu du début. Il vaut donc mieux désactiver la résolution HD avant de commencer à jouer.

Réflexion et récapitulation

1. Les jeunes peuvent créer une affiche avec Canva pour enseigner des pratiques cybersécuritaires à leurs amis et à leur famille. Conseil : Montrez-leur comment créer et personnaliser un projet dans l'outil.
    a. ***Remarque :*** Les élèves peuvent partager leur projet avec des collègues afin de pouvoir travailler en équipe.
2. Discutez des différentes professions présentées à l'annexe A, Liens avec des professions.
3. Encouragez les élèves à devenir des ambassadrices et des ambassadeurs cyberfutés en transmettant à leur famille et à leurs amis les stratégies apprises durant cette activité (et leur affiche).

Recommandations selon le mode d'enseignement

Ce contenu a été conçu pour l'enseignement en personne, mais peut être présenté dans d'autres contextes. Voici des recommandations pour l'enseigner à distance (en ligne) ou dans un environnement « débranché » (avec peu ou pas de support technologique).

À distance (en ligne)	Débranché (Peu ou pas de techno)
Généralités	
• Invitez les jeunes à ouvrir leur micro ou à utiliser la boîte de clavardage, à leur convenance. • Utilisez un outil permettant à tous les élèves de participer aux	• Utilisez un tableau pour faire des remue-méninges et noter les idées et réponses des jeunes.

À distance (en ligne)	Débranché (Peu ou pas de techno)
discussions en ligne (Mentimeter, Jamboard, etc). • Notez les liens à fournir aux élèves et copiez-les dans la boîte de clavardage au moment opportun. • Faites appel à des sondages ou à d'autres formes d'interactions en groupe pour faire le point avec les élèves et maintenir leur niveau de motivation.	
Introduction	
• L'exercice peut être réalisé tel quel en ligne. Le remue-méninges peut se faire verbalement ou au moyen d'un outil de collaboration (Jamboard, Google Doc, Mentimeter, etc.).	• Décrivez ou imprimez l'image.
1. Les cyberarnaques	
• Sélectionnez l'option Pointeur laser lors de la présentation des diapositives. • L'exercice peut être réalisé tel quel en ligne. Le remue-méninges peut se faire verbalement ou au moyen d'un outil de collaboration (Jamboard, Google Doc, Mentimeter, etc.).	• Imprimez les exemples inclus dans la présentation afin que les élèves puissent les analyser.

À distance (en ligne)	Débranché (Peu ou pas de techno)
2. Les pratiques cybersécuritaires	
• Affichez un chronomètre virtuel (avec décompte) sur votre écran afin que les élèves sachent combien de temps il leur reste à jouer. • Faites une démonstration du jeu à votre écran avant de laisser les jeunes jouer par eux-mêmes.	• Plateau de jeu Sécurise ton réseau (voir l'annexe C) : décrivez les règles du jeu à l'aide de la présentation Règles du jeu Sécurise ton réseau. • Remettez un plateau de jeu à chaque élève (ou à chaque équipe, selon le cas). • Les élèves peuvent jouer plusieurs fois de suite (le but étant de bien saisir les différents termes utilisés). • À la fin du jeu, demandez aux élèves de fournir leur score final (plus leur score est élevé, plus leur réseau est sécuritaire).
Réflexion et récapitulation	
• Les jeunes peuvent concevoir leur affiche sur Canva ou sur papier.	• Les jeunes peuvent concevoir leur affiche sur papier plutôt que d'utiliser Canva.

Possibilités d'adaptation

Il est possible d'adapter différents aspects de cette activité (durée, environnement, matériel, taille du groupe ou instructions) pour la rendre plus accessible ou plus complexe. Les **modifications** ci-dessous vous permettront de diminuer le niveau de difficulté de l'activité et les **ajouts**, d'augmenter sa durée ou son niveau de difficulté.

Modifications

GÉNÉRALITÉS

- Sélectionnez l'option de sous-titrage (si disponible) pour la diffusion des vidéos.
- Fournissez une souris aux jeunes pour faciliter l'utilisation de l'ordinateur portable.
- Faites travailler les élèves en équipes de deux ou plus plutôt qu'individuellement.

1. LES CYBERARNAQUES

- Remplissez le questionnaire sur l'hameçonnage (ou au moins une question) avec toute la classe.
- Examinez seulement une partie des exemples fournis dans la présentation et/ou faites travailler les élèves en équipes.

2. LES PRATIQUES CYBERSÉCURITAIRES

- Jouez à La rivière de la réalité avec toute la classe ou faites une courte démonstration avant de laisser les élèves jouer.
    - La deuxième question est minutée. Cela pourrait être stressant pour les jeunes qui ont besoin de plus de temps pour lire ou écrire.

Ajouts

1. LES CYBERARNAQUES

- Jouez à Missing Link Game (Texas A&M University) (en anglais).

RÉFLEXION ET RÉCAPITULATION

- Les élèves peuvent créer une affiche avec Canva afin de faire connaître à leurs amis et à leur famille les pratiques cybersécuritaires à adopter lorsqu'on interagit avec de nouvelles personnes en ligne. Transmettez-leur ce lien utile

https://www.canva.com/fr_fr/affiches/modeles/campagne-affichage/ et explorez vous-même toutes les possibilités de cet outil.

- Montrez rapidement aux jeunes comment créer et personnaliser un projet dans Canva. Si cela facilite l'activité, sélectionnez vous-même un modèle sur la plateforme plutôt que de laisser ce choix aux élèves ou de les laisser dessiner leur propre affiche.
- Les élèves peuvent concevoir leur affiche sur papier plutôt que d'utiliser Canva.
- Si le temps le permet, invitez les élèves à présenter leur affiche à la classe.

Références et remerciements

Binary Tattoo. (19 juin 2017). *Glossary of Internet Scams and Fraud Terminology*. https://www.binarytattoo.com/glossary-of-internet-fraud-and-scam-terminology/

BleepingComputer. (11 janvier 2018). *Remove the Amazon Rewards Event Web Page*. https://bit.ly/37piROX

Canva. (s. d.) *Créer une affiche*. https://www.canva.com/fr_fr/creer/posters/

Centre canadien pour la cybersécurité. (Avril 2020). *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*. https://www.cyber.gc.ca/fr/orientation/ne-mordez-pas-lhamecon-reconnaitre-et-prevenir-les-attaques-par-hameconnage

Centre canadien pour la cybersécurité. (s. d.). *Glossaire*. https://cyber.gc.ca/fr/glossaire

Centre de la sécurité des télécommunications. (19 juin 2020). Pensez cybersécurité | Hameçonnage: ne mordez pas! [Vidéo]. https://www.youtube.com/watch?v=MxmIPP3AbLM

Common Sense Education. (11 janvier 2019). *Teen Voices: Oversharing and Your Digital Footprint* [Vidéo]. https://www.youtube.com/watch?v=ottnH427Fr8

Federal Trade Commission Consumer Information. (Mai 2019). *How to Recognise and Avoid Phishing Scams*. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Goodwill Community Foundation. (s. d.). *What is Clickbait?* https://edu.gcfglobal.org/en/thenow/what-is-clickbait/1/

Google for Education. (25 juin 2017). *Stay Safe from Phishing and Scams* [Vidéo]. https://www.youtube.com/watch?v=R12_y2BhKbE

IBMorg. (22 janvier 2020). *5 Tips for Cybersecurity Safety brought to you by Mayim Bialik* [Vidéo]. https://www.youtube.com/watch?v=ZOtQ21hXJ7k

Imperva. (s. d.). *Phishing Attacks*. https://www.imperva.com/learn/application-security/phishing-attack-scam/

Kapersky. (s. d.). *What is VPN? How It Works, Types of VPN*. https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

NOVA Labs. (s. d.). *Cybersecurity Lab*. https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Panda Security. (2 avril 2019). *10 Social Media Scams and Hot to Spot them*. https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/

PCS Business Systems. (s. d.). *Malware, phishing, spyware and viruses - what's the difference?* https://www.pcs-systems.com/different-cyber-threats/

Security Boulevard. (26 novembre 2019). *Dropbox Phishing Scam: Don't Get Fooled*

by Fake Shared Documents. https://securityboulevard.com/2019/11/dropbox-phishing-scam-dont-get-fooled-by-fake-shared-documents/

Search Security. (2014). *Phishing Definition*. https://searchsecurity.techtarget.com/definition/phishing

Tech Radar. (14 novembre 2017). *You need a VPN when accessing public Wi-Fi - here's why.* https://www.techradar.com/news/public-wi-fi-and-why-you-need-a-vpn

Tech Xplore. (27 mars 2020). *Router phishing scam targets global fear over coronavirus).* https://techxplore.com/news/2020-03-router-phishing-scam-global-coronavirus.html

Windsor Public Library. (16 février 2017). *Spotting a Phishing Attempt*. https://www.windsorpubliclibrary.com/?p=47291

Annexes

Annexe A : Liens avec des professions

GENDARMERIE ROYALE DU CANADA : ANALYSTE DE RENSEIGNEMENTS EN CYBERCRIMINALITÉ

- L'analyste de renseignements en cybercriminalité élabore des stratégies pour cerner les types de cybercrimes et les tendances en la matière. Elle ou il utilise cette information pour concevoir des outils de renseignement stratégique et pour fournir son avis lors d'enquêtes criminelles complexes.

SPÉCIALISTE EN CYBERSÉCURITÉ (SPÉCIALISTE EN SÉCURITÉ DE L'INFORMATION)

- La ou le spécialiste en cybersécurité repère les vulnérabilités des systèmes informatiques et des logiciels ainsi que les menaces visant ceux-ci. Elle ou il élabore des mesures de sécurité et des solutions afin de protéger les systèmes contre les cybercrimes tels que le piratage et les logiciels malveillants. Ces mesures et solutions peuvent prendre la forme de technologies ou de processus organisationnels.

ANALYSTE EN CYBERSÉCURITÉ (ANALYSTE EN SÉCURITÉ DE L'INFORMATION)

- L'analyste en cybersécurité surveille les réseaux et les systèmes informatiques d'une entreprise et protège ceux-ci contre les menaces et les brèches informatiques en élaborant et implantant des mesures de sécurité.

DÉVELOPPEUSE, DÉVELOPPEUR DE LOGICIELS DE SÉCURITÉ

- La développeuse ou le développeur de logiciels de sécurité conçoit et implante des outils de sécurité logicielle, développe des systèmes et teste la vulnérabilité de tous ces outils et systèmes.

Annexe B : Information documentaire

Binary Tattoo propose un excellent glossaire pour se familiariser avec les fraudes Internet et les cyberarnaques : Glossary of Internet Fraud and Scam Terminology (en anglais).

L'HAMEÇONNAGE

Selon le Centre canadien pour la cybersécurité, l'hameçonnage est une attaque dans le cadre de laquelle un cybercriminel vous contacte (par téléphone, texto, courriel ou média social) pour vous inciter à divulguer des renseignements personnels, à cliquer sur un lien malveillant ou à télécharger un logiciel malveillant. Les tentatives d'hameçonnage prennent souvent la forme d'un message générique distribué en masse par une source qui semble légitime et fiable (école, institution financière, etc.). Selon l'étendue de l'information divulguée ou de l'accès fourni, l'hameçonneur pourrait mettre la main sur de nombreux renseignements confidentiels à votre sujet (numéro de téléphone, adresse, date d'anniversaire, informations bancaires, etc.) et utiliser ceux-ci pour voler votre identité, vos mots de passe ou votre argent.

Centre canadien pour la cybersécurité (avril 2020). *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*. Source : https://www.cyber.gc.ca/fr/orientation/ne-mordez-pas-lhamecon-reconnaitre-et-prevenir-les-attaques-par-hameconnage

Les trois principales raisons d'hameçonner :

1) Accéder à des comptes ou à des renseignements.
2) Voler de l'argent en s'emparant d'informations de carte de crédit ou bancaires, ou encore en utilisant un rançongiciel pour bloquer l'accès à un appareil ou à un système.
3) Provoquer le chaos afin de semer le trouble.
    a) L'hameçonnage vise à vous faire divulguer des renseignements personnels afin de nuire à vos finances ou à votre réputation, ou encore d'endommager les systèmes auxquels vous avez accès (entreprises, école, etc.).

Voici certains indices d'hameçonnage à surveiller :

- On invente un prétexte pour vous inciter à cliquer sur un lien ou à ouvrir une pièce jointe.
    - Exemples : pour réclamer un remboursement, faire un paiement, confirmer des renseignements personnels, régler un problème avec le compte.
    - Prend souvent la forme de courriels contenant des liens vers des sites web malveillants.
- Formule de salutation générique (p. ex. « Bonjour utilisateur »).
- Vous ne reconnaissez pas le nom, l'adresse courriel, ni le numéro de téléphone de l'expéditeur.
- Le courriel semble provenir d'une entreprise que vous connaissez (auprès de laquelle vous avez ou non un compte).
- Le message contient beaucoup de fautes d'orthographe et de grammaire.
- L'expéditeur demande des renseignements personnels ou confidentiels.
- La demande est urgente et comporte une échéance.
    - Le message semble provenir d'une connaissance, mais l'objet de la demande est étrange et ne correspond pas à ce que vous envoie habituellement cette personne.
- L'offre présentée semble trop belle pour être vraie.

Voici certains conseils utiles pour vous protéger contre les tentatives d'hameçonnage (sources : Centre canadien pour la cybersécurité et Federal Trade Commission) :

- Protégez vos appareils à l'aide d'un logiciel de sécurité (mis à jour automatiquement).
- Protégez vos comptes au moyen de l'authentification multifacteur.
- Vérifiez les liens avant de cliquer dessus.
- Évitez de transmettre des renseignements sensibles par courriel ou par texto.
- Appelez l'expéditeur pour vérifier sa légitimité (p. ex. si vous recevez un appel d'un conseiller de votre institution financière, raccrochez et rappelez-le).
- Filtrez les pourriels.
- Limitez l'information que vous divulguez en ligne (p. ex. les numéros de téléphone et de postes des employés).

LES LOGICIELS MALVEILLANTS

Selon le Centre canadien pour la cybersécurité, un logiciel malveillant sert à infiltrer et à endommager un système informatique, parfois sans que l'utilisateur en soit conscient. Lors d'un hameçonnage, les arnaqueurs cherchent à vous convaincre de cliquer sur un lien ou de télécharger un fichier infecté par un logiciel malveillant afin de s'emparer de votre identité, de vos mots de passe ou de votre argent.

Types de logiciels malveillants :

- **Logiciel espion :** difficile à détecter, recueille de l'information sans qu'on s'en rende compte.
- **Virus :** programme qui se reproduit dans la mémoire d'un ordinateur et se propage.
- **Ver informatique :** s'exécute et se reproduit par lui-même pour causer des dommages (p. ex. supprimer des fichiers ou envoyer des documents à partir du courriel de l'utilisateur).
- **Cheval de Troie :** se dissimule sous les apparences d'un logiciel légitime.
- **Rançongiciel :** chiffre des fichiers et oblige l'utilisateur à payer pour retrouver l'accès à ceux-ci.

LE PIÈGE À CLICS

Le piège à clics est une forme trompeuse de publicité conçue pour attirer votre attention et vous convaincre de cliquer sur quelque chose. Il peut s'agir d'un titre qui suscite l'émotion ou la curiosité pour vous amener à cliquer sur un article, une image ou une vidéo.

Le terme « piège à clics » désigne toute pratique qui consiste à utiliser un titre accrocheur pour inciter les internautes à cliquer sur un contenu (p. ex. « Les médecins détestent le truc anti-âge de cette femme. Découvrez pourquoi! »). La publicité recourt souvent à cette technique, et pas forcément à des fins malfaisantes. **Cependant, dans certains cas, le piège à clics fait partie d'une stratégie élaborée pour arnaquer les gens (p. ex. en les dirigeant vers un site contenant un logiciel malveillant ou en les amenant à faire un don à un faux organisme de bienfaisance).**

Les sites web qui font usage de pièges à clics accordent souvent plus d'importance au nombre de visites qu'à la qualité et à la crédibilité de l'information qu'ils publient. Combinés avec les fausses nouvelles, les pièges à clics peuvent se propager rapidement dans les médias sociaux et avoir un effet néfaste.

Selon la Goodwill Community Foundation (Learn Free) (en anglais), voici comment reconnaître un piège à clics :

- Titre souvent choquant.
- Titre et image vagues qui stimulent l'imagination (p. ex. « Tu ne croiras jamais ce que ce professeur a dit durant son cours! »).
- Titre qui vous dit quoi ressentir.

Annexe C : Autres ressources

INTRODUCTION

Image

- Image piège à clics

1. LES CYBERARNAQUES

Présentation PowerPoint

- Les cyberarnaques : hameçonnage et piège à clics

Vidéo

- Stay Safe from Phishing and Scams (Google for Education, 3:14, sous-titres en français)

Site web

- Questionnaire sur l'hameçonnage

2. LES PRATIQUES CYBERSÉCURITAIRES

Image

- Plateau de jeu Sécurise ton réseau

Présentation PowerPoint

- Règles du jeu Sécurise ton réseau

Vidéo

- 5 Tips for Cybersecurity Safety brought to you by Mayim Bialik (IBMorg, 5:45, sous-titres en français)

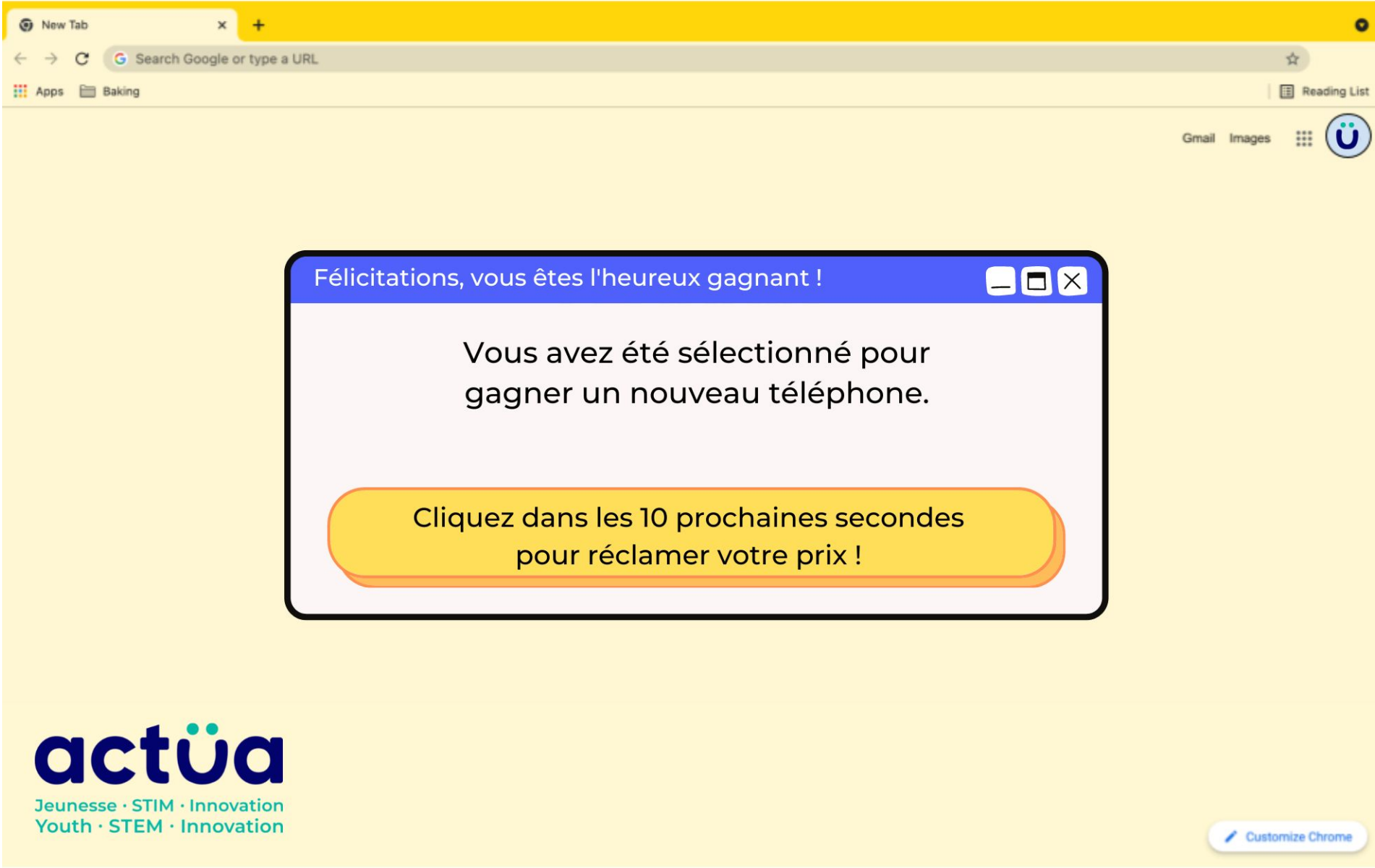
Site web

- Interland de Google (La rivière de la réalité)

RÉFLEXION ET RÉCAPITULATION

Site web

- Outil de création d'affiches Canva


New Tab
Search Google or type a URL
Apps
Baking
Reading List
Gmail
Images
Félicitations, vous êtes l'heureux gagnant !
Vous avez été sélectionné pour gagner un nouveau téléphone.
Cliquez dans les 10 prochaines secondes pour réclamer votre prix !
actüa
Jeunesse · STIM · Innovation
Youth · STEM · Innovation
Customize Chrome

DÉPART	Tu as téléchargé l'antivirus Norton Security, qui, hereusement, a empêché un virus d'infecter ton ordinateur. **+5 points**	Tu as divulgé ton mot de passe lors d'un hammeçonnage. Mets à jour touts tes mots de passe et rapporte la cyberanaque aux autorités! **-2 points**	Tu obtiens un serveur **+1 point**	Un ver informatique a détruit les fichiers stockés sur ton ordinateur. N'oublie pas d'installer un coupe-feu pour empêcher que ça se reproduise! **-2 points**	
Un virus t'empêche d'utiliser ton ordinateur. Tu aurais dû installer un antivirus et le mettre à jour régulièrement. **-5 points**	Tu obtiens un serveur **+1 point**	Tu as reçu un courriel t'annonçant que tu avais gagné un ordinateur portable. En cliquant sur le lien dans le courriel, tu as téléchargé accidentellement un virus. **-2 points**	Tu n'as pas accédé à tes comptes pendant que tu utilisais le Wi-Fi du centre commercial. **+2 points**	Tu obtiens une base de données **+1 point**	**-2 points**
	Tu t'es rendu compte qu'un hameçonneur tentait d'obtenir ta date d'anniversaire et ton adresse. Tu as signalé la tentative aux autorités. **+5 points**	Un virus a infecté ton disque dur parce que ton antivirus n'était pas à jour. N'oublie pas de toujours faire les mises à jour! **-2 points**	Tu obtiens un coupe-feu **+1 point**	Tu obtiens un support de stockage **+1 point**	
Ton serveur a planté! Tu retournes à la case départ (et tu perds tous tes points).	En tentant de télécharger un jeu gratuit, tu as plutôt téléchargé un logiciel malveillant. N'oublie pas d'y penser à deux fois avant de cliquer sur un lien! **-5 points**	Erreur de base de données **-1 point**	Tu as accidentellement téléchargé un logiciel malveillant sur ton ordinateur, mais comme tu sauvegardes fréquemment tes données, tu n'as pas eu à payer pour pouvoir retrouver l'accès à tes fichiers. **+1 point**	Tu obtiens un base de données **+1 point**	Tu as accidentellement activé un cheval de Troie en cliquant sur une application qui avait l'air d'être un jeu. **-3 points**
	Erreur de coupe-feu **-1 point**	Tu obtiens un serveur **+1 point**	Afin de réclamer un soi-distant prix, tu remplis un formulaire provenant d'un expéditeur inconnu et tu télécharges un rançongiciel. N'oublie pas de rester à l'affût des pourriels! **-5 points**	Tu vérifies toujours tes courriels pour t'assurer qu'il ne s'agit pas de pourriels déguisés. **+2 points**	
ARRIVÉE	Avant de télécharger quelque chose, tu as vérifié la source et constaté qu'elle n'était pas fiable. Tu as évité de télécharger un cheval de Troie sur ton ordinateur. Bravo, œil de lynx! **+3 points**	Tu as téléchargé illégalement un film contenant un virus et maintenant ton navigateur est envahi de publicités. Prends garde à ce que tu fais en ligne! **-5 points**	Tu obtiens un support de stockage **+1 point**	Tu as téléchargé illégalement un film contenant un virus et maintenant ton navigateur est envahi de publicités. Prends garde à ce que tu fais en ligne! **-5 points**	