

**PROGRAMME D'EMPLOYABILITÉ  
DES JEUNES EN MATIÈRE DE  
COMPÉTENCES POUR RÉUSSIR**



**COMPÉTENCES  
NUMÉRIQUES  
D'ACTIVITÉ**



  
**SkillsCompétences  
Canada**

A blue, jagged-edged starburst shape containing the logo and text for SkillsCompétences Canada. The logo icon depicts a stylized hand holding a leaf or flame.

## Remerciements

Les cahiers d'activités du programme *Compétences pour réussir pour les jeunes prêts à travailler* ont été créés par *Skills/Compétences Canada*, avec le soutien du gouvernement du Canada.

Nous tenons à remercier tout particulièrement *Bow Valley College* qui a participé à l'élaboration du contenu des cahiers d'activités.

Nous avons veillé à utiliser tout le matériel reproduit conformément aux lignes directrices sur l'utilisation équitable et aux politiques et procédures en matière de propriété intellectuelle de *Bow Valley College*. Le matériel n'est utilisé qu'à des fins non commerciales. Tous les coûts associés à l'accès aux cahiers d'exercices seront limités au recouvrement des coûts pour l'impression et les services associés. La reproduction, quel que soit le moyen utilisé, ou la copie du matériel sans autorisation, est strictement interdite.

Droit d'auteur © *Skills/Compétences Canada 2017*  
Tous droits réservés.

Pour plus d'informations, veuillez contacter :  
*Skills/Compétences Canada*

294, rue Albert, bureau 201 | Ottawa (Ontario) | K1P 6E6

Télécopieur : 613-691-1404 |

Numéro sans frais : 1 877-754-5226

<https://skillscompétencescanada.com/fr>

Ce document est distribué par *Skills/Compétences Canada*.

Financé en partie par le gouvernement  
du Canada par le biais du programme  
de Compétence pour réussir

**Canada**

# COMPÉTENCES NUMÉRIQUES

Utilise la table des matières pour naviguer dans ce cahier d'activités. Suis ta progression en cochant chaque sujet terminé.

PARTIE ET SUJET		Page	√
Bienvenue ; L'histoire des compétences pour réussir ; Les choses à savoir au sujet du calcul		5	
<b>EXERCISES!</b>		<b>29</b>	
1	Les métiers spécialisés se transforment grâce au numérique !	31	
2	Mots de passe et cybersécurité	45	
3	Gérer les médias sociaux avec intelligence	57	
4	Questions d'argent en ligne	71	
5	Utiliser l'IA	85	
6	La santé numérique	101	
<b>AMPLIFICATEUR!</b>		<b>119</b>	
1	Amplificateur de compétences numériques – vie privée en ligne et cybersécurité	121	
2	Amplificateur de compétences numériques – un court historique des mots de passe	125	
<b>RÉPONSES!</b>		<b>129</b>	
0	Associations de tâches et de compétences	131	
1	Les métiers spécialisés se transforment grâce au numérique !	133	
2	Mots de passe et cybersécurité	139	
3	Gérer les médias sociaux avec intelligence	145	
4	Questions d'argent en ligne	149	
5	Utiliser l'IA	157	
6	La santé numérique	163	
<b>QUESTIONS POUR TESTER TES COMPÉTENCES!</b>		<b>171</b>	
1	Compétences Numériques : Questions pour tester tes compétences	173	
2	Compétences Numériques : Questions pour tester tes compétences – Réponses	179	





**BIENVENUE AU PROGRAMME COMPÉTENCES POUR RÉUSSIR POUR LES JEUNES PRÊTS À TRAVAILLER**



**Q : COMMENT UTILISER CE CAHIER D'ACTIVITÉS?**

**1**

COMMENCE PAR JETER UN COUP D'ŒIL AUX INFORMATIONS ET AUX ANECDOTES SUR COMPÉTENCES NUMÉRIQUES ET LES COMPÉTENCES POUR RÉUSSIR.

**2**

EXERCE-TES COMPÉTENCE À L'AIDE DE LA SECTION « EXERCICES ».

**3**

TRAVAILLE TES COMPÉTENCES À L'AIDE DE LA SECTION « AMPLIFICATION ».

**4**

VÉRIFIE TON TRAVAIL À L'AIDE DE LA SECTION « RÉPONSES! ».

**5**

ESSAIE DE RÉPONDRE AUX QUESTIONS À LA FIN POUR VOIR SI TES COMPÉTENCES SONT SOLIDES.



## INTRODUCTION AUX COMPÉTENCES POUR RÉUSSIR



**LES COMPÉTENCES POUR RÉUSSIR SONT  
LES COMPÉTENCES DONT TOUT LE MONDE A BESOIN  
POUR TRAVAILLER, APPRENDRE ET VIVRE.  
ELLES FORMENT LA BASE POUR APPRENDRE  
D'AUTRES COMPÉTENCES.**





## LES NEUF COMPÉTENCES POUR RÉUSSIR



Les Compétences pour réussir sont une des composantes principales des Initiatives de Skills/Compétences Canada. Regardons tout cela d'un peu plus près.

### LES NEUF COMPÉTENCES POUR RÉUSSIR :

 ADAPTABILITY ADAPTABILITÉ	 COLLABORATION COLLABORATION	 COMMUNICATION COMMUNICATION	 CREATIVITY & INNOVATION CRÉATIVITÉ ET INNOVATION	 DIGITAL COMPÉTENCES NUMÉRIQUES
 NUMERACY CALCUL	 PROBLEM SOLVING RÉSOLUTION DE PROBLÈMES	 READING LECTURE	 WRITING RÉDACTION	



## MESURER LES COMPÉTENCES POUR RÉUSSIR

Pensez à une fois où vous avez essayé quelque chose de nouveau; ce peut être un sport, apprendre à coder ou à jouer d'un instrument. Vous avez peut-être été très bon tout de suite, mais la plupart d'entre nous ne le sont pas. Nous devons nous exercer pour nous améliorer. De la même manière, vous devez vous exercer pour développer vos Compétences pour réussir. Pour faire cela, vous devez vous exercer à faire des tâches, répondre à des questions et résoudre des problèmes liés aux Compétences pour réussir, en commençant par celles du niveau débutant pour passer aux tâches des niveaux intermédiaire et avancé.

NIVEAUX DES COMPÉTENCES POUR RÉUSSIR		
Débutant	Intermédiaire	Avancé
Besoin de s'exercer	Prêt à continuer à apprendre	Prêt à partir!

Les compétences, comme nos muscles, se renforcent au fur et à mesure que nous les utilisons. Renforcer tes compétences pour réussir t'aidera à réussir dans le milieu du travail en constante évolution de nos jours et dans la vie de tous les jours.

Que représentent ces niveaux

- Les tâches, questions et problèmes du niveau débutant sont moins difficiles que ceux des niveaux intermédiaire et avancé.
- Les personnes dont les compétences sont au niveau débutant doivent s'exercer pour les renforcer. Lorsque tes compétences atteignent ou dépassent le niveau intermédiaire, elles sont assez solides pour te permettre de développer des compétences scolaires, techniques ou professionnelles.
- Les employeurs préfèrent embaucher des travailleurs efficaces, capables de travailler et d'apprendre, car ils savent qu'ils pourront mieux résoudre des problèmes avec précision, terminer leur travail, apprendre de nouveaux procédés et de s'adapter aux changements au travail.
- Ces compétences sont aussi importantes dans la vie quotidienne. Nous avons tous besoin de lire des informations, remplir des documents, prendre des décisions budgétaires, travailler, communiquer de manière efficace avec nos amis, notre famille, nos enseignants et nos employeurs, et utiliser des ordinateurs et d'autres technologies numériques.

**LES COMPÉTENCES POUR RÉUSSIR SONT IMPORTANTES.**

**LES COMPÉTENCES POUR RÉUSSIR SERVENT DANS LA VIE DE TOUS LES JOURS ET AU TRAVAIL. ELLES NOUS AIDENT À CONTINUER À APPRENDRE POUR NE PAS ÊTRE LAISSÉ DE CÔTÉ.**



**À TON TOUR! ESSAIE DE TROUVER LA TÂCHE QUI CORRESPOND À LA COMPÉTENCE**

Regarde la liste ci-dessous. De quelles compétences penses-tu avoir besoin pour terminer chacune des tâches? Écris l'abréviation de chacune des compétences que tu juges nécessaire pour terminer chacune des tâches. Un exemple t'est donné dans le tableau. (PETIT CONSEIL : toutes les tâches utilisent plus d'une compétence.)



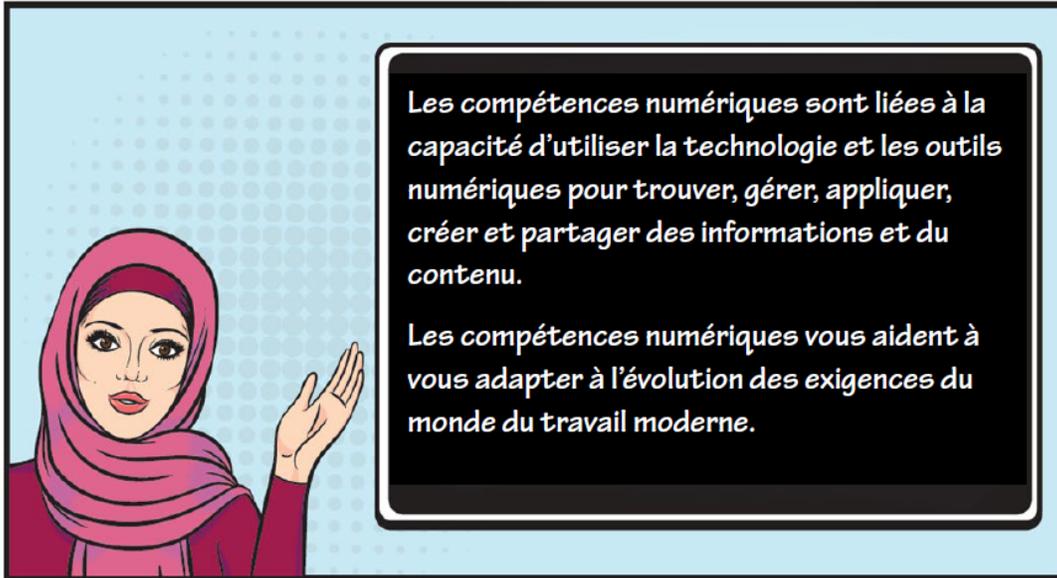
Tâche	Compétences utilisées
Trouver les informations en ligne pour programmer un nouvel iPhone	
Faire une demande de permis d'apprenti conducteur en ligne	
Acheter des billets pour un concert en ligne	
Aider à organiser une activité de collecte de fonds pour votre équipe sportive	
Préparer un plan pour vous acheter les bottes que vous voulez quand vous vous rendez compte qu'elles sont plus chères que prévu.	
Trouver un autre moyen de transport lorsque vous ne pouvez pas utiliser la voiture pour aller skier	
Envoyer un texto à ton entraîneur pour lui dire que tu seras en retard à ton entraînement, lui expliquer pourquoi et comment tu vas rattraper ce que tu auras manqué.	
Arriver de bonne heure au bureau pour que ton patron t'enseigne à utiliser le nouveau système de paiement	CAL
Regarder les horaires des transports en commun en ligne pour arriver à l'heure à ton nouveau travail	

Compétences pour réussir	
ADA	Adaptabilité
COL	Collaboration
COM	Communication
CI	Créativité et innovation
CN	Compétences numériques
C	Calcul
RP	Résolution de problèmes
L	Lecture
R	Rédaction





## PARLONS DE COMPÉTENCES NUMÉRIQUES



### AU SUJET DES COMPÉTENCES NUMÉRIQUES

Chaque jour, vous êtes confronté à de nouveaux défis à l'école, au travail ou dans la vie quotidienne. Bon nombre de ces défis exigent que vous utilisiez vos compétences numériques. Le mot « numérique » est un terme générique qui englobe les outils que vous utilisez (téléphones portables, tablettes, etc.), les façons dont vous créez et gérez les informations sur ces outils (logiciels, applications, feuilles de calcul, etc.) et les connaissances que vous utilisez pour faire tout cela en toute sécurité.

Les raisons pour lesquelles le « numérique » est souvent au centre de l'attention sont nombreuses. En voici quelques-unes. Le monde est tellement connecté que les nouvelles sont disponibles presque en temps réel. Les activités que nous effectuons tous les jours — comme le magasinage, l'utilisation du téléphone ou les opérations bancaires — nous obligent de plus en plus à interagir avec la technologie numérique. La technologie a un impact sur tous les aspects de notre vie et le rythme des changements numériques s'accélère.

Une personne née après 2001 est souvent appelée « un enfant du numérique », c'est-à-dire une personne qui a été élevée à l'ère de la technologie numérique et qui est donc familiarisée avec les ordinateurs et Internet depuis son plus jeune âge. Cependant, le fait d'être familier ne signifie pas automatiquement que l'on sait comment utiliser cette technologie de manière sûre et intelligente. N'oubliez pas que pour utiliser les informations et les outils numériques en toute sécurité, il est essentiel d'être toujours au courant de l'évolution de la technologie et des menaces éventuelles pour la vie privée et la sécurité. Demeurez vigilant !



## LE NUMÉRIQUE FAIT UNE DIFFÉRENCE



### DES COMPÉTENCES POUR LE PRÉSENT ET L'AVENIR

La technologie numérique a changé la manière dont vous trouvez et partagez les informations, résolvez les problèmes et communiquez avec les autres. La plupart des emplois font maintenant appel à des compétences numériques, et vous en avez besoin lorsque vous appliquez d'autres compétences telles que la lecture, l'écriture ou le calcul.

<https://srdc.org/project/research-report-to-support-the-launch-of-skills-for-success-structure-evidence-and-recommendations-final-report/#>

## VOS COMPÉTENCES NUMÉRIQUES COMPRENNENT VOTRE CAPACITÉ À COMPRENDRE ET À APPLIQUER TOUTES LES CATÉGORIES SUIVANTES D'OUTILS ET DE PRATIQUES NUMÉRIQUES.



### APPAREILS

Ceux-ci incluent les ordinateurs, les tablettes, les téléphones, les ordinateurs de poche et des outils spécifiques à certains métiers



### OUTILS

Cela inclut connaître les façons d'utiliser les logiciels, les applications, intelligence artificielle (IA), etc.



### DONNÉES ET INFORMATIONS

Cela inclut connaître les façons pour rechercher, évaluer et organiser des données numériques.



### COLLABORATION

Cela inclut l'utilisation d'outils pour communiquer, collaborer et partager de l'information.



### PRATIQUES SÉCURITAIRES

Celles-ci incluent la capacité de comprendre et de mettre en application les règlements liés à la confidentialité et la sécurité.



### APPRENTISSAGE

Cela inclut la capacité de la capacité à suivre l'évolution rapide des technologies pour faire évoluer ses compétences numériques existantes.



**ESSAYONS MAINTENANT D'UTILISER DES COMPÉTENCES NUMÉRIQUES**

Réfléchissez à la manière dont vous utilisez vos compétences numériques tous les jours, que ce soit dans le cadre de votre travail ou dans votre vie quotidienne. Complétez le tableau suivant en donnant des exemples de la manière dont vous accomplissez des tâches numériques ou pratiquez la sécurité numérique liée à chaque catégorie, que ce soit au travail ou dans la vie quotidienne. Soyez aussi précis que possible. Nous avons ajouté des exemples de la manière dont un maçon utilise ses compétences numériques pour vous aider.



<b>CATÉGORIES NUMÉRIQUES</b>	<b>MAÇON</b>	<b>VOUS</b>
Appareils	<i>Utilise des outils de mesure numériques pour calculer avec précision la surface et le nombre de pavés nécessaires.</i>	
Outils	<i>Utilise les courriels pour confirmer les dépenses et envoie des textos à ses collègues.</i>	
Informations et données	<i>Saisit des informations dans un gabarit sous forme de feuille de calcul pour préparer un devis.</i>	
Collaboration	<i>Il envoie un texto à son superviseur s'il est en retard ou s'il va arriver en avance.</i>	
Pratiques sécuritaires	<i>Utilise un mot de passe pour accéder au système de comptabilité de l'entreprise afin de mettre à jour les informations personnelles du client en toute sécurité.</i>	



Apprentissage	<i>Participe à des cours en ligne pour mettre à jour ses compétences en matière de sécurité ou apprendre à réaliser des aménagements paysagers avec des briques.</i>	
---------------	--	--



## LES COMPÉTENCES NUMÉRIQUES FONT UNE DIFFÉRENCE

### AU TRAVAIL

Lorsque vous travaillez, vos compétences numériques sont un facteur important pour réussir. De nombreux métiers spécialisés qui étaient autrefois considérés comme essentiellement « manuels » exigent aujourd'hui des compétences numériques poussées. Prenons l'exemple des outils de diagnostic qu'utilisent aujourd'hui les techniciens de l'automobile et de l'équipement lourd, et le fait qu'on lit désormais les schémas sur des tablettes plutôt que sur des rouleaux de papier. Votre sécurité, votre productivité et vos possibilités d'avancement seront toutes touchées par vos compétences numériques.



### À LA MAISON

Notre vie privée est également touchée par nos compétences numériques. La façon dont nous communiquons avec les autres, que ce soit par texto, par courriel ou par des applications de messagerie, nous oblige tous à utiliser des compétences numériques. Naviguer dans les tâches numériques telles que l'envoi de textos et les achats en ligne peut vous sembler facile, mais il est essentiel de vous assurer que vous effectuez ces tâches en toute sécurité pour protéger votre sécurité personnelle et financière, ainsi que la vie privée des personnes avec lesquelles vous communiquez.

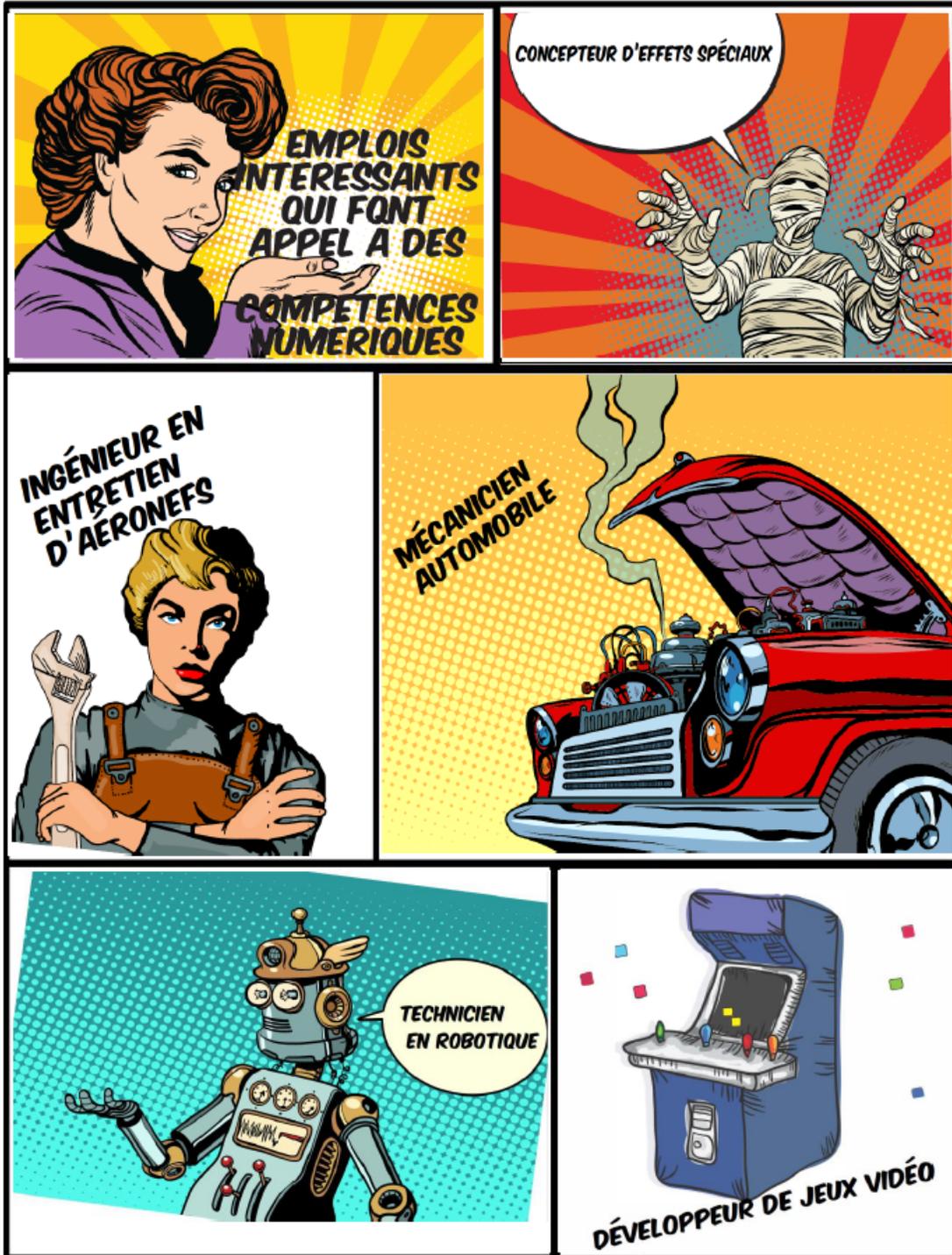
### MESURER LES COMPÉTENCES NUMÉRIQUES

Les compétences numériques sont mesurées en fonction de trois niveaux :

- Niveau de base : vous pouvez utiliser les fonctions de base des appareils numériques qui vous sont familiers. Vous avez besoin d'être guidé pour trouver et évaluer la pertinence et la fiabilité des informations en ligne, et pour vous utiliser des pratiques en ligne sûres.
- Niveau intermédiaire : Vous pouvez utiliser un plus grand nombre de fonctions d'appareils numériques familiers ou non, y compris les personnaliser à des fins spécifiques (par exemple, télécharger et utiliser une application, créer des macros pour automatiser des tâches). Vous pouvez trouver et utiliser des informations en ligne pertinentes et fiables et vous utiliser des pratiques en ligne sûres.
- Niveau avancé : Vous avez une connaissance approfondie du fonctionnement des appareils numériques et des systèmes de technologie de l'information. Vous pouvez trouver et utiliser des informations en ligne pertinentes et fiables pour améliorer les processus numériques, y compris votre propre sécurité en ligne. Vous pouvez évaluer vos besoins numériques futurs et maintenir vos propres compétences numériques à jour.



**EMPLOIS INTÉRESSANTS QUI FONT APPEL À DES COMPÉTENCES NUMÉRIQUES**





## UNE LEÇON NUMÉRIQUE...

### Au sujet des applications

Une application est un logiciel créé pour accomplir une tâche spécifique pour un utilisateur ou, parfois, pour un autre logiciel. À l'origine, le terme « application » désignait principalement les applications mobiles axées sur un seul objectif ou une seule tâche, comme consulter la météo, prendre des notes ou effectuer des calculs. Au fil du temps, la signification du terme s'est élargie et il est aujourd'hui généralement utilisé pour désigner les applications fonctionnant sur n'importe quel type d'appareil.



Les applications mobiles sont pratiques à utiliser et très efficaces. Les expériences personnalisées qu'elles offrent les rendent très attrayantes pour les utilisateurs.

### Les applications les plus populaires en 2022

TikTok a été l'application la plus populaire au monde, selon le nombre de téléchargements en 2022, conservant son titre pour la quatrième année consécutive. La plateforme vidéo a enregistré 672 millions de téléchargements en 2022, et l'entreprise a également doublé son chiffre d'affaires annuel pour atteindre 9,4 milliards de dollars, selon *Business of Apps*.

<https://www.visualcapitalist.com/cp/most-popular-apps-by-downloads/>

### Les applications d'IA deviennent rapidement populaires

En 2020 et 2021, de nombreuses applications professionnelles essentielles, telles que Zoom et Microsoft Teams, ont connu une croissance rapide et un succès énorme. Alors que les téléchargements de ces applications ont diminué en 2022, de nombreuses autres applications axées sur les voyages, la nourriture et le magasinage, comme Google Maps, McDonald's et Shein, ont aidé à combler le vide.

Toutefois, ce sont les applications d'intelligence artificielle (IA), dont Lensa AI et ChatGPT, qui ont connu le plus grand succès vers la fin de l'année dernière. Ces mêmes applications infusées par l'IA pourraient-elles devenir les chefs de file en matière de téléchargements pour les applications les plus populaires de l'avenir ?

<https://www.visualcapitalist.com/cp/most-popular-apps-by-downloads/>

### Un conseil utile

Le nettoyage de vos applications facilitera la navigation sur votre téléphone, améliorera sa performance et le rendra plus sûr. Les anciennes applications qui ne sont plus pertinentes ou que vous n'avez pas mises à jour depuis un certain temps peuvent créer de graves problèmes de sécurité. [consumercellular.com](https://www.consumercellular.com)



## UNE LEÇON NUMÉRIQUE...

### LE PARTAGE DANS LES MÉDIAS SOCIAUX



Si vous vous sentez obligé de partager des nouvelles ou des informations ou de participer à des discussions en ligne, voici qui peut être utile, et même important. Ce type de discussion est l'une des choses pour lesquelles les médias sociaux étaient initialement prévus. Mais si vous décidez de participer, rendez service à vous-même et à ceux qui liront vos messages en prenant le temps de confirmer que les informations que vous partagez sont exactes. Vérifiez celles-ci auprès d'au moins une autre source digne de confiance. Le temps de plus que vous prendrez pourrait faire la différence entre un ajout utile à une discussion importante et l'ajout de bruit et de chaos mal informés.

Comme l'a écrit Charlie Warzel, collaborateur de The Atlantic : « La plus grande force des médias sociaux est donc son péché originel : ces sites sont excellents puisqu'ils vous donnent l'impression d'être connectés et informés, souvent au détriment de l'information réelle ».

<https://www.theatlantic.com/technology/archive/2023/10/social-media-infrastructure-news-algorithms/675714/>



**LE NUMÉRIQUE FAIT UNE DIFFÉRENCE...**

**VOUS CROYEZ QUE LE NUMÉRIQUE A PEU D'IMPORTANCE ? PENSEZ-Y À NOUVEAU !**



**DEUX ÉLÉMENTS CLÉS À RETENIR D'UN RAPPORT PUBLIÉ EN SEPTEMBRE 2020 PAR LE CONFERENCE BOARD DU CANADA :**

1. L'amélioration des compétences numériques sera le facteur le plus important pour adapter les métiers spécialisés du Canada à l'avenir du travail.

Le rapport décrit quelques-unes des façons dont la technologie numérique a un impact sur les métiers et ce que cela signifie pour les compétences spécifiques que les apprentis et les gens qui travaillent dans les métiers doivent développer.

Les métiers du secteur de l'automobile. Les mécaniciens d'entretien, les spécialistes de l'équipement lourd, les réparateurs et les techniciens en carrosserie, ainsi que les métiers liés à la force motrice sont touchés par l'évolution vers des systèmes plus informatisés et la disparition du travail mécanique. Les mécaniciens d'entretien automobile sont les plus touchés par les changements technologiques sur leur lieu de travail, par rapport à d'autres grands métiers du Sceau rouge. L'utilisation accrue de la numérisation dans les métiers de l'automobile



reflète le passage aux véhicules électriques, hybrides et autopilotés. On s'attend également à ce que les mécaniciens d'entretien automobile aient besoin de compétences en matière d'interface homme-machine pour réparer les véhicules autopilotés.

Les métiers du secteur de la fabrication. Les soudeurs, les machinistes, les mécaniciens industriels et les autres artisans de l'industrie s'appuient de plus en plus sur des technologies sophistiquées. Ils travaillent avec des thermostats numériques, des systèmes de contrôle numériques, des capteurs, des outils de mesure numériques et des systèmes d'automatisation.

Les métiers du secteur de la construction. Les électriciens du bâtiment, les plombiers, les charpentiers, les monteurs de charpentes métalliques, les mécaniciens en réfrigération et en climatisation, et d'autres corps de métier de la construction sont touchés par une dépendance croissante aux technologies intelligentes, à la modélisation des informations sur le bâtiment, aux systèmes d'automatisation et à l'Internet des objets, tels que les systèmes d'éclairage domestique personnalisés qui sont accessibles à partir d'un téléphone intelligent.

Les métiers du secteur des services alimentaires. Les cuisiniers, les boulangers et les chefs utilisent des applications numériques et des systèmes informatisés dans leur travail quotidien. La paie et la planification sont plus souvent effectuées à l'aide des applications, la technologie point de vente rend le service plus rapide, et les commandes se font sur des sites Web ou à l'aide de chèques électroniques.

2. Les gens travaillant dans les métiers auront besoin de sept compétences numériques de base.

1. Technique
2. Gestion de l'information
3. Communication numérique
4. Collaboration virtuelle
5. Créativité
6. Esprit critique
7. Résolution de problèmes dans les environnements numériques

**VOS COMPÉTENCES NUMÉRIQUES SONT-ELLES PRÊTES ?**



## LES COMPÉTENCES NUMÉRIQUES EN ACTION !



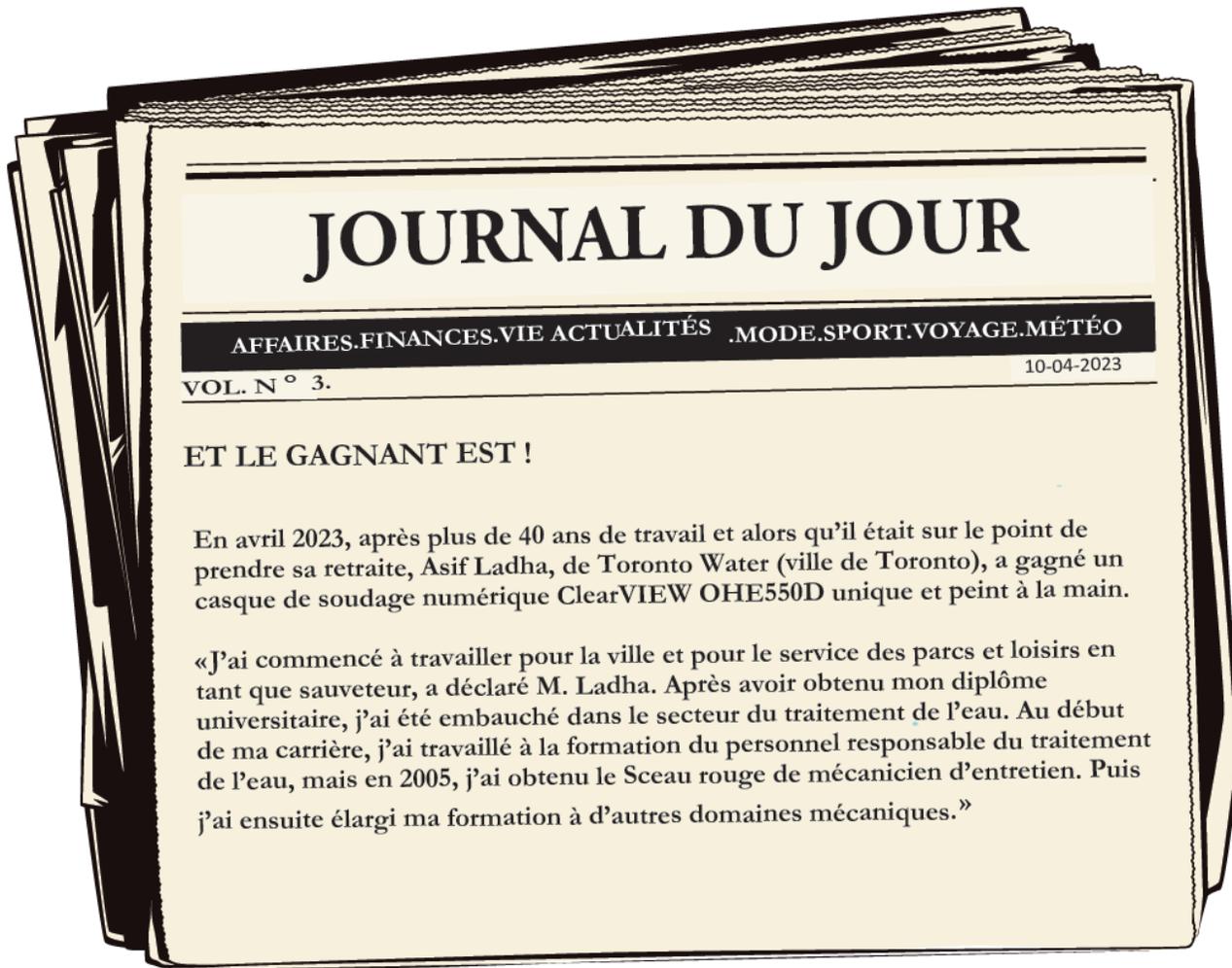
1. Les mécaniciens en réfrigération et en climatisation utilisent des bases de données pour saisir les informations concernant le contrat du client et le numéro de modèle des systèmes de chauffage et de ventilation installés. (Compétences numériques, niveau de base)
2. Les installateurs électriques consultent des sites Web et naviguent dans plusieurs menus pour trouver des données techniques telles que l'affectation des broches sur les puces de circuits intégrés. (Compétences numériques, niveau intermédiaire)
3. Les peintres d'automobiles utilisent des baguettes électroniques portatives pour effectuer un balayage des couleurs de peinture des véhicules et déterminer les couleurs et les codes de peinture. (Compétences numériques, niveau intermédiaire)
4. Les cuisiniers utilisent des feuilles de calcul pour déterminer les quantités de chaque ingrédient nécessaires pour préparer 20 commandes plutôt qu'une en utilisant des formules. (Compétences numériques, niveau intermédiaire)
5. Les graphistes utilisent des logiciels de CAO (conception assistée par ordinateur) pour produire des animations informatiques dans les films et les jeux. Par exemple, les animateurs 2D et 3D utilisent la CAO pour créer des bâtiments et des structures rigides ou les scènes d'arrière-plan des jeux. (Compétences numériques, niveau intermédiaire)
6. Les testeurs électroniques utilisent des logiciels de test automatisés ou des multimètres et oscilloscopes numériques informatisés. (Compétences numériques, niveau intermédiaire)

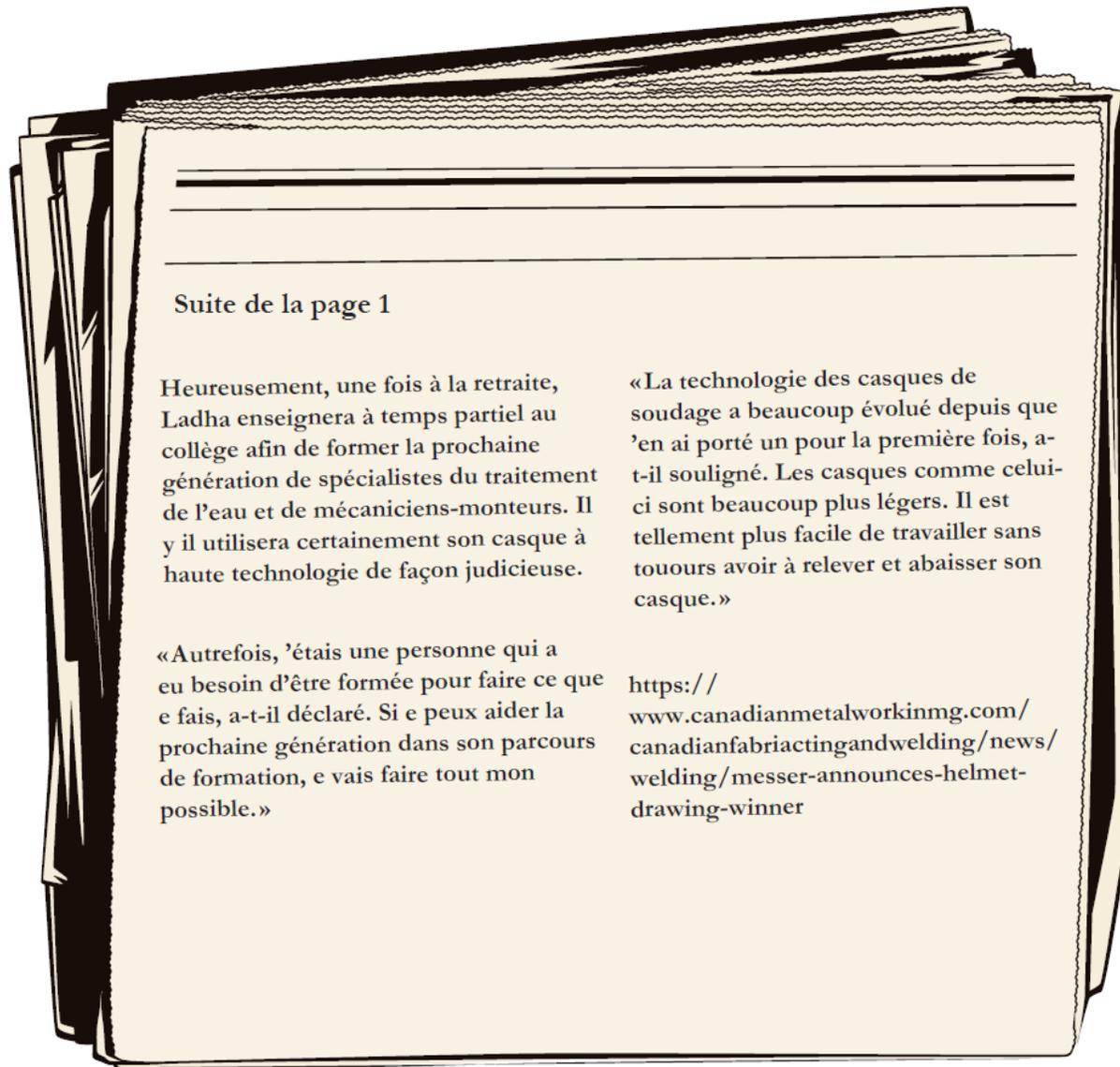


- 7.** Les soudeurs saisissent des données et font fonctionner des machines de découpe au plasma, des soudeuses orbitales et d'autres équipements commandés par ordinateur. (Compétences numériques, niveau intermédiaire)
  
- 8.** Les charpentiers utilisent des équipements commandés par ordinateur tels que des stations totales, des niveaux intelligents et des systèmes d'alarme sur le lieu de travail. (Compétences numériques, niveau de base)
  
- 9.** Les technologues de l'aérospatiale utilisent des bases de données pour optimiser le flux de travail, par exemple en utilisant un logiciel de planification de l'entretien des avions d'entreprise pour accéder aux calendriers d'entretien exigés par les fabricants. (Compétences numériques, niveau intermédiaire)
  
- 10.** Les concepteurs de sites Web utilisent des logiciels graphiques pour créer des bannières, des arrière-plans, des illustrations, des animations et d'autres éléments de conception à utiliser dans les sites Web. (Compétences numériques, niveau avancé)



**LES COMPÉTENCES NUMÉRIQUES À LA UNE !**







## LES COMPÉTENCES NUMÉRIQUES EN PETITES BOUCHÉES

### LES COMPÉTENCES NUMÉRIQUES À HOGWARTS (POUDLARD)

On utilisait des mots de passe dans tout le château de Hogwarts pour restreindre l'accès à certaines zones, comme les salles communes des maisons et les bureaux des professeurs. Les mots de passe à Hogwarts semblaient changer souvent.

Pendant la période où Sir Cadogan gardait la salle commune de Gryffindor, il changeait si souvent de mot de passe que Neville Longbottom devait les noter. Cette liste a été volée par Crookshanks et remise à Sirius Black, ce qui lui a permis d'entrer dans la salle.

On utilisait aussi des mots de passe pour accéder à l'émission de radio Potterwatch, afin de la protéger de l'écoute éventuelle des Death Eaters (Mangemorts). On annonçait de nouveaux mots de passe à la fin de chaque émission, ce qui permettait aux auditeurs d'écouter l'émission suivante. <https://harrypotter.fandom.com/wiki/Password>



### UNE PERSONNE MOYENNE A 100 MOTS DE PASSE DIFFÉRENTS !



Selon Nordpass, les trois mots de passe les plus utilisés sont les suivants :

- Password (5 millions d'utilisateurs)
- 123 456 (1,5 million)
- 123 456 789 (plus de 410 000)

18 % des employés partagent leurs mots de passe avec d'autres personnes. Le partage de mots de passe

est une erreur courante qui peut gravement compromettre la cybersécurité d'un organisme. Mais pourquoi les employés agissent-ils ainsi ? Des études ont montré que 42 % des travailleurs déclarent le faire pour collaborer plus facilement avec les membres de leur équipe, et que 38 % déclarent partager leurs mots de passe parce que c'est la politique de l'entreprise.

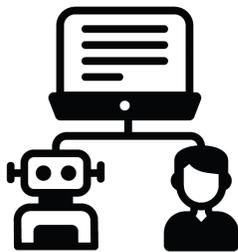
<https://blog.entrustit.co.uk/6-facts-about-passwords-that-will-make-you-think>



## LES COMPÉTENCES NUMÉRIQUES EN PETITES BOUCHÉES

### LE TEST DE TURING

Le test de Turing a été mis au point dans les années 1950 par Alan Turing, mathématicien, informaticien, logicien, cryptanalyste, philosophe et biologiste théorique britannique, après qu'il eut passé plusieurs années à apprendre le concept d'apprentissage automatique. Turing pensait qu'un ordinateur pouvait être qualifié d'intelligent s'il était capable d'imiter les réactions humaines dans des conditions spécifiques. En d'autres termes, un ordinateur est intelligent s'il est capable de penser.



Turing Test

Le test implique deux personnes : un interrogateur (A) et un joueur (B), ainsi qu'un ordinateur (C), tous situés dans des pièces différentes. L'interrogateur pose aux deux joueurs (un humain et un ordinateur) une série de questions écrites et tente de déterminer quel joueur est l'humain et quel joueur est l'ordinateur. Si l'interrogateur ne parvient pas à déterminer lequel des deux joueurs est l'humain, on déclare l'ordinateur vainqueur. On dit alors que la machine est capable de penser et qu'elle a gagné le « jeu de l'imitation ».



Nommé ou récompensé aux *Oscars*, aux *Golden Globe Awards*, aux *Screen Actors Guild Awards* et au *People's Choice Award* lors de la 39<sup>e</sup> édition du Festival international du film de Toronto, *Imitation Game (The Imitation Game)* est un film à suspense très réussi réalisé en 2014 et basé sur la vie d'Alan Turing.

Le titre du film cite le nom du jeu proposé par le cryptanalyste Alan Turing pour répondre à la question « Les machines peuvent-elles penser ? »

Le cinéma, y compris ces films terrifiants et à succès, s'intéresse depuis longtemps à la question de savoir ce qui se passe lorsque des personnages dotés d'intelligence artificielle deviennent des méchants et se retournent contre leurs créateurs.

- Matrix (*The Matrix*)
- 2001 : L'Odyssée de l'espace (*2001 : A space Odyssey*)
- Terminator (*The Terminator*)



## LES COMPÉTENCES NUMÉRIQUES EN PETITES BOUCHÉES

### SE SOUVENIR DE L'ORIGINE DES MÉTIERS

Les outils manuels ou électriques que les générations précédentes d'artisans utilisaient sont de plus en plus remplacés par des versions numériques dans votre génération. Respecter et apprécier l'évolution de son métier est un élément important de la vie professionnelle. Le Musée canadien de la fabrication a rassemblé des machines et des outils qui ont été créés et utilisés entre 1750 et 1920 au Canada, en Grande-Bretagne, aux États-Unis et en Afrique.



En plus des outils, le musée conserve une petite collection de véhicules tels que des automobiles, des camions, des motocyclettes, des tracteurs à vapeur et des véhicules tirés par des chevaux. Tous les outils et machines ont été soigneusement préservés et remis en état de fonctionnement. L'objectif du musée est de créer et de maintenir une source d'information précise sur les

machines pour tous ceux qui partagent cet intérêt. Il est possible de voir les outils en visitant le musée à Calgary, en Alberta, ainsi qu'en ligne dans les pages de la galerie des collections.

<https://museumofmaking.org/gallery/>.

### LA GÉNÉRATION Z ET LA VIE PRIVÉE

Selon un article de blogue de [Malwarebytes.com](https://malwarebytes.com), la génération Z « ... se soucie de la vie privée d'une manière différente... La génération Z s'inquiète le plus de l'exposition de ses informations privées à cause du risque de harcèlement, d'intimidation et de perte d'amis. En fait, lorsqu'il s'agit de nombreuses inquiétudes relatives à la vie privée qui sont liées à la cybersécurité, la génération Z s'en soucie moins dans l'ensemble. Selon notre étude, contre 51 % des personnes n'appartenant pas à la génération Z, 62 % des membres de la génération Z sont d'accord ou tout à fait d'accord avec l'affirmation suivante :

« Je suis plus inquiet de voir mes informations privées exposées en ligne (par exemple, des photos ou des vidéos embarrassantes ou compromettantes, des informations sur ma santé mentale ou ma sexualité, etc.) que des menaces habituelles en matière de cybersécurité (comme les virus, les logiciels malveillants, etc.) »

[https://www.malwarebytes.com/blog/personal/2023/11/what-gen-z-really-cares-about-when-it-comes-to-](https://www.malwarebytes.com/blog/personal/2023/11/what-gen-z-really-cares-about-when-it-comes-to-privacy?utm_source=iterable&utm_medium=email&utm_campaign=b2c_pro_oth_20231106_novemberweeklynewsletter_v1_169927472188&utm_content=person_with_their_long_hair)

[privacy?utm\\_source=iterable&utm\\_medium=email&utm\\_campaign=b2c\\_pro\\_oth\\_20231106\\_novemberweeklynewsletter\\_v1\\_169927472188&utm\\_content=person\\_with\\_their\\_long\\_hair](https://www.malwarebytes.com/blog/personal/2023/11/what-gen-z-really-cares-about-when-it-comes-to-privacy?utm_source=iterable&utm_medium=email&utm_campaign=b2c_pro_oth_20231106_novemberweeklynewsletter_v1_169927472188&utm_content=person_with_their_long_hair)



## LES COMPÉTENCES NUMÉRIQUES EN PETITES BOUCHÉES

### SOUFFREZ-VOUS DE CYBERCHONDRIE ?



La cyberchondrie est une forme de maladie connue comme un trouble anxieux. Le terme a été inventé au début des années 2000 comme un type d'hypocondrie lié aux recherches en ligne. La cyberchondrie se définit par la recherche compulsive sur Internet d'informations au sujet de symptômes réels ou imaginaires d'une maladie.

### LA TECHNOLOGIE FAIT MAL

Souffrez-vous de douleurs physiques liées à l'utilisation excessive de vos appareils technologiques ? Le « pouce texto », la « main iPad » et le « coude égoportrait (selfie) » sont de véritables blessures physiques que de nombreuses personnes, et en particulier, les plus jeunes, signalent de plus en plus souvent à leur professionnel de la santé. Il s'agit de variantes de ce que l'on appelle les microtraumatismes répétés. Comme leur nom l'indique, ces blessures sont causées parce que l'on effectue les mêmes actions encore et encore, parfois des centaines, ou même des milliers, de fois par jour. L'utilisation d'un ordinateur ou d'un téléphone intelligent peut nous placer dans des positions non naturelles pendant de longues périodes. L'important est d'être à l'écoute de son corps et, lorsque vous sentez que quelque chose vous fait mal, d'arrêter de le faire pendant un certain temps.





## LES COMPÉTENCES NUMÉRIQUES EN PETITES BOUCHÉES

### OUVREZ LA BOUCHE ET DITES « AI ? »

Une brosse à dents dotée d'une intelligence artificielle ? L'ajout de l'IA vise à améliorer les choses. Aujourd'hui, il existe même une brosse à dents qui utilise l'intelligence artificielle pour améliorer la façon dont vous vous brossez les dents. Une brosse à dents à intelligence artificielle est programmée pour prendre les données de milliers de brossages enregistrés en laboratoire, les combiner avec votre style de brossage personnel et formuler des recommandations pour rendre votre sourire encore plus blanc. Le système vous avertit si vous avez oublié des endroits lors du brossage ou si vous ne vous brossez pas assez longtemps. Et, bien sûr, une application pour téléphone intelligent vous permet de suivre vos progrès en matière de brossage.





# **METS TES COMPÉTENCES AU TRAVAIL!**

**METS TES COMPÉTENCES AU TRAVAIL DANS CETTE PARTIE DU CAHIER D'ACTIVITÉS. LES COMPÉTENCES SONT COMME LES MUSCLES: PLUS ON LES EXERCE ET PLUS ELLES DEVIENNENT FORTES. FAIS TRAVAILLER LES MUSCLES DE TES COMPÉTENCES POUR REUSSIR EN FAISANT TOUS CES EXERCICES DE MANIÈRE AUTONOME. VÉRIFIE SI TU AS BIEN COMPRIS À L'AIDE DU CAHIER DE RÉPONSES.**

# COMPÉTENCES NUMÉRIQUES

Utilise la table des matières pour naviguer dans ce cahier d'activités. Suis ta progression en cochant chaque sujet terminé.

PARTIE ET SUJET		Page	√
<b>EXERCICES!</b>		<b>29</b>	
1	Les métiers spécialisés se transforment grâce au numérique !	31	
2	Mots de passe et cybersécurité	45	
3	Gérer les médias sociaux avec intelligence	57	
4	Questions d'argent en ligne	71	
5	Utiliser l'IA	85	
6	La santé numérique	101	



## 1. LES MÉTIERS SPÉCIALISÉS SE TRANSFORMENT GRÂCE AU NUMÉRIQUE !

La transformation numérique des métiers spécialisés signifie que les travailleurs de ces métiers ont besoin d'un ensemble de compétences élargi. Les deux grandes catégories d'outils numériques dans les métiers sont 1) les outils utilisés dans de nombreux métiers et 2) les outils spécifiques à des métiers particuliers.

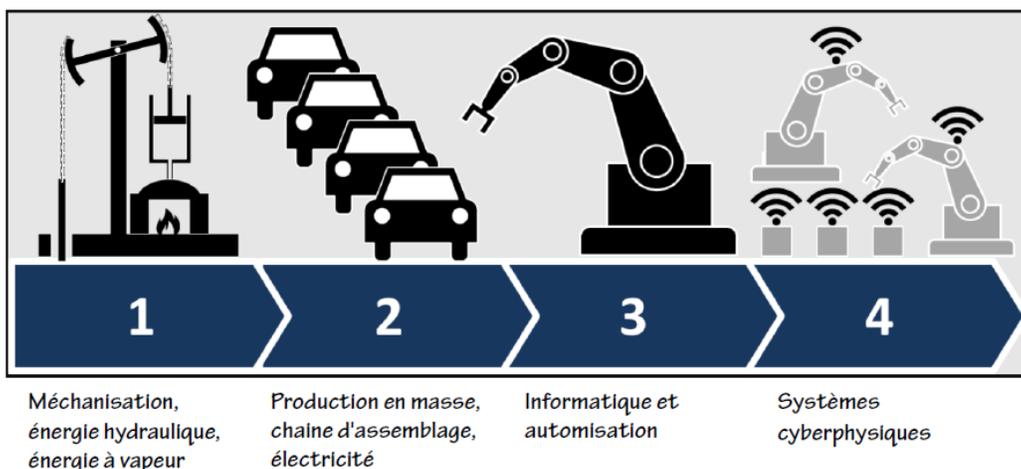
### Outils numériques pour tous les métiers

Presque tous les corps de métier utilisent des outils numériques pour la planification, la facturation et d'autres logiciels pour accélérer leur travail administratif. Les téléphones intelligents et les plateformes de communication telles que Zoom et Slack permettent une plus grande collaboration et une capacité accrue à résoudre les problèmes entre les gens de métier, les concepteurs et les ingénieurs. Les dessins schématiques utilisés dans de nombreux métiers sont désormais lus sur des tablettes plutôt que sur des rouleaux de plans en papier.

### Outils numériques propres à un métier

Parmi les exemples d'outils numériques spécifiques aux métiers, on peut citer les outils de diagnostic utilisés aujourd'hui par les techniciens de l'automobile et de l'équipement lourd, ainsi que l'excavation guidée par GPS, couramment utilisée dans les projets de construction de routes et d'extraction des ressources naturelles.

Cette transformation numérique fait partie de ce que l'on appelle la quatrième révolution industrielle.



Les quatre révolutions industrielles. Tiré de Wikipedia Commons. (Christoph Roser at AllAboutLean.com 2015)



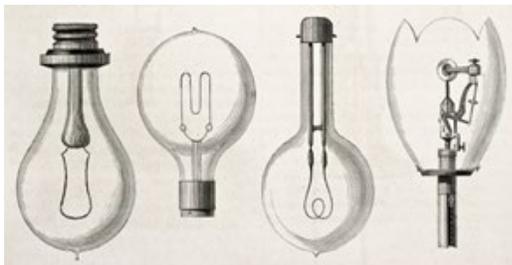
## Les quatre révolutions industrielles

### La (première) révolution industrielle

La première révolution industrielle est communément appelée « la révolution industrielle » ou « l'ère de la vapeur ». Elle est liée à la mécanisation et au passage d'un monde agricole à un monde industriel. Elle a débuté à la fin du XVIII<sup>e</sup> siècle. Elle se caractérise par l'introduction de machines à eau et à vapeur dans l'industrie manufacturière. Le moteur à vapeur, l'industrie textile et le génie mécanique en sont les aspects fondamentaux. Elle a duré de la fin du XVIII<sup>e</sup> au début du XIX<sup>e</sup> siècle. L'année 1784, au cours de laquelle le premier métier à tisser mécanique a été construit, est souvent citée comme le point de départ de cette révolution.



### La deuxième révolution industrielle



La deuxième révolution industrielle, également appelée « l'ère de l'électricité », a introduit la production de masse. Elle est liée à l'utilisation intensive de l'énergie électrique et se produit entre la fin du 19<sup>e</sup> et le début du 20<sup>e</sup> siècle (1870-1900). Elle est marquée par l'introduction de l'électricité et du pétrole dans la production de masse et par le développement du chemin de fer et de l'acier. L'année 1870, au cours de laquelle la première chaîne de montage a été

utéchelle dans les abattoirs, est parfois citée comme date de début de l'ère industrielle.

### La troisième révolution industrielle

La caractéristique principale de la troisième révolution industrielle, ou « l'ère de l'information » a été la numérisation généralisée (informatisation). C'est le début de la première génération de technologies de l'information et des communications (TIC) dans l'industrie. Également appelée « Industrie 3.0 », elle a débuté au milieu du XX<sup>e</sup> siècle, dans les années 1960, et a coïncidé avec la nouvelle ère de l'industrialisation, la quatrième révolution industrielle. Elle se caractérise par l'utilisation de l'électronique et des technologies de l'information au sein de l'industrie. Le premier contrôleur logique programmable (CLP) a introduit l'ordinateur personnel dans la production commerciale en 1969.





## La quatrième révolution industrielle



La quatrième révolution industrielle, également appelée « l'ère numérique », la révolution digitale ou « Industrie 4.0 », se caractérise par la capacité à connecter des objets réels + des personnes + des objets virtuels à l'aide d'un réseau numérique. Elle a pour élément clé le changement profond des systèmes de fabrication grâce à l'intégration des TIC, et de l'Internet des objets (Ido). Le début du 21<sup>e</sup> siècle en constitue le point de départ. La quatrième révolution industrielle a chevauché en douceur la

troisième. Certains chercheurs pensent que le terme « évolution » est plus approprié que celui de « révolution » pour désigner les changements en cours, car les principaux éléments existaient déjà et seuls quelques nouveaux développements ont été ajoutés. Dans les deux cas, la principale transformation réside dans le fait que la production est devenue numérique.

Édité (puis traduit) à partir du texte suivant : [https://www.researchgate.net/figure/The-four-industrial-revolutions-From-the-Wikimedia-Commons-Christoph-Roser-at\\_fig1\\_335581542](https://www.researchgate.net/figure/The-four-industrial-revolutions-From-the-Wikimedia-Commons-Christoph-Roser-at_fig1_335581542)

### Surveillez les dates !

Le 18<sup>e</sup> siècle = 1701-1800

Le 19<sup>e</sup> siècle = 1801-1900

Le 20<sup>e</sup> siècle = 1901-2000

Le 21<sup>e</sup> siècle = 2001-2100

### Industrie 5.0 approche !

Le Japon et la Commission européenne ont identifié une possible cinquième révolution axée non seulement sur la technologie numérique, mais aussi sur la manière dont cette technologie peut être utilisée pour améliorer la société. Pour les travailleurs, Industrie 5.0 signifie laisser l'automatisation et les robots accomplir des tâches répétitives tout en les libérant pour d'autres activités.



À l'aide des informations contenues dans l'article portant sur les quatre révolutions industrielles, complétez le tableau afin de mieux comprendre les principaux changements survenus au cours de chacune des révolutions. Cochez le numéro de la révolution qui correspond à chaque affirmation. (*Compétences numériques, niveau intermédiaire*)

DESCRIPTEUR DE LA RÉVOLUTION INDUSTRIELLE	1 <sup>re</sup>	2 <sup>e</sup>	3 <sup>e</sup>	4 <sup>e</sup>
Également appelée l'ère de l'électricité				
A considérablement modifié l'industrie textile				
Également appelée l'ère numérique				



A commencé au milieu du 20 <sup>e</sup> siècle				
L'économie est passée de l'agriculture à l'industrie				
Début des chaînes d'assemblage				
L'utilisation des ordinateurs a commencé				
Les machines fonctionnent à l'aide de moteurs à l'eau ou à la vapeur				
Évolution de la 3 <sup>e</sup> révolution				
Également appelée l'ère de l'information				
Début de la production de masse				
A eu lieu au cours des 18 <sup>e</sup> et 19 <sup>e</sup> siècles				
L'impact sur les métiers se poursuit au 21 <sup>e</sup> siècle				
A considérablement modifié l'industrie du chemin de fer				

Chacune de ces quatre révolutions, ou plutôt des évolutions a apporté des changements significatifs à la fois pour les métiers spécialisés et dans la façon dont vous accomplissez vos activités quotidiennes. Les recherches menées par le Centre des compétences futures indiquent que les travailleurs qualifiés ont désormais besoin de sept compétences numériques de base :

- des compétences techniques,
- la gestion de l'information,
- la communication numérique,
- la collaboration virtuelle,
- la créativité,
- la pensée critique et
- la résolution de problèmes dans les environnements numériques.

## LES COMPÉTENCES AU TRAVAIL

Mike Bocsik est un technicien en réparation automobile qui possède des dizaines d'années d'expérience en tant que gérant de sa propre entreprise et 12 autres années d'expérience en tant qu'instructeur automobile chargé de former des apprentis techniciens en réparation automobile.

Son expérience montre que les étudiants d'aujourd'hui veulent s'impliquer pleinement dans ce qu'ils apprennent et sont avides de connaissances approfondies, de détails et d'informations sur les développements les plus récents du secteur.

<https://www.cbc.ca/news/canada/skilled-trades-education-1.6773564>



Cela inclut des informations sur l'évolution des outils numériques qu'ils doivent utiliser dans le cadre de leur travail.

Pour les techniciens en réparation automobile, être compétent sur le plan numérique signifie combiner leur connaissance des véhicules avec la capacité d'effectuer des tâches telles que :

- Utiliser un téléphone intelligent pour prendre des photos de pièces usées pour les clients afin de montrer pourquoi une pièce doit être remplacée ou prendre une photo d'un numéro VIN pour rechercher des pièces avec précision.
- Accéder à des informations pertinentes sur des forums en ligne ou sur YouTube et les évaluer pour dépanner des réparations de véhicules.
- Interpréter les informations provenant d'outils de diagnostic et de numériseurs sur Internet.

Source : Centre des compétences futures

Skills/Compétences Canada identifie les compétences numériques comme l'une des trois principales compétences pour réussir dont ont besoin les techniciens en réparation automobile et les mécaniciens d'entretien, reconnaissant que les véhicules d'aujourd'hui sont devenus des ordinateurs sur roues.

**1.** Dans la colonne N° de tâche du tableau, inscrivez les numéros des tâches de travail qui correspondent aux outils numériques pour lesquels ils sont le plus souvent utilisés. L'une d'entre elles est déjà effectuée pour vous. (*Compétences numériques, niveau intermédiaire*)

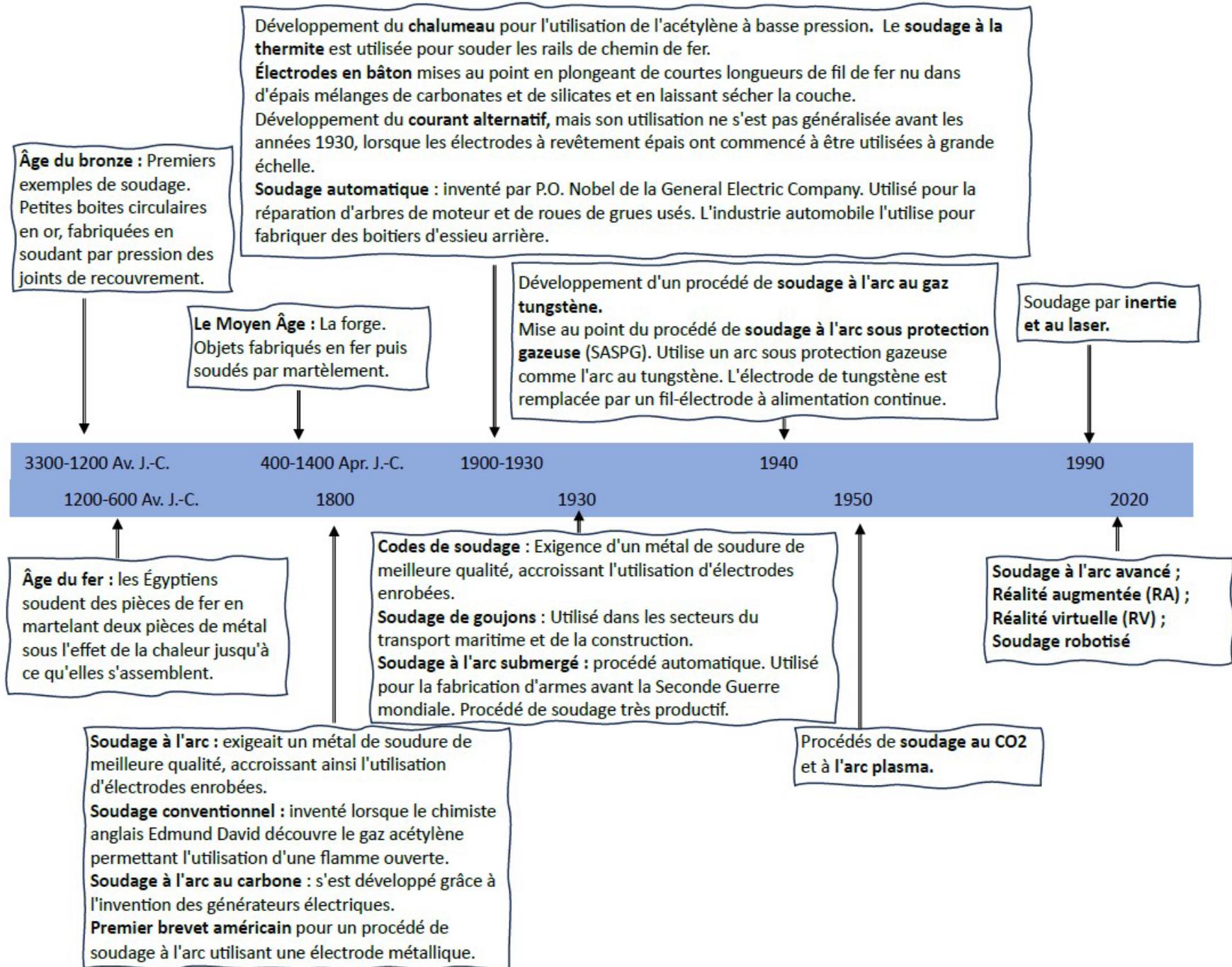
Outil numérique	N° de tâche	Tâche au travail
Traitement de texte		1. Effectuer des relevés d'énergie électrique.
Logiciel de tableur		2. Effectuer des réparations complètes.
Logiciel de communication	8	3. Télécharger des données destinées à réguler les paramètres de fonctionnement d'un véhicule.
Logiciel de dessin		4. Accéder à des données telles que les codes d'erreur des ordinateurs de bord.
Bases de données		5. Rédiger des lettres aux courtiers d'assurance pour leur présenter les résultats des inspections mécaniques.



Internet		6. Utiliser le logiciel graphique intégré aux outils de balayage pour accéder aux affichages de données de l'oscilloscope, tels que les valeurs des signaux et les schémas d'allumage de l'oscilloscope.
Multimètre (peut mesurer plusieurs propriétés électriques)		7. Effectuer des relevés énergétiques et dépister les problèmes.
Équipement électronique		<del>8. Échanger des courriels avec d'autres techniciens dans d'autres lieux.</del>
Outils de balayage tels que les oscilloscopes (affichent des signaux électriques et montrent comment les signaux évoluent dans le temps)		9. Récupérer les informations sur les réparations et les dessins techniques.
Ordinateurs portables connectés à des modules de commande logique numérique (contrôleurs programmables qui permettent aux machines d'exécuter des processus sans intervention humaine)		10. Participer aux cours de formation et aux séminaires proposés par les fournisseurs et les employeurs.
Équipements informatisés tels que les machines de réglage de la trajectoire des roues		11. Enregistrer et suivre les heures facturables.

Source : <https://www.skillscompetencescanada.com/wp-content/uploads/2021/02/Automove-Service-PDF.pdf>

## Chronologie du développement du soudage





## DÉVELOPPEMENTS NUMÉRIQUES DANS LE DOMAINE DU SOUDAGE

Comme le montre la chronologie de la page précédente, les outils utilisés pour le soudage ont considérablement évolué depuis les premiers outils manuels de base et le feu jusqu'à l'introduction de batteries, d'électrodes, de systèmes automatiques et, aujourd'hui, de développements numériques faisant appel à l'intelligence artificielle (IA).



Complétez les affirmations suivantes à l'aide des informations contenues dans la chronologie.  
(Compétences numériques, niveau intermédiaire)

1. Le soudage à l'arc au carbone fonctionne à l'aide de générateurs \_\_\_\_\_.
2. Le soudage de goujons a d'abord été utilisé dans les secteurs \_\_\_\_\_ et \_\_\_\_\_.
3. Durant le processus de soudage \_\_\_\_\_, l'arc se déplace entre deux électrodes de carbone.
4. Au cours des années \_\_\_\_\_, on note plusieurs développements importants dans le domaine de la soudure ; la création de \_\_\_\_\_ de soudage, le soudage de goujons et le soudage à l'arc \_\_\_\_\_.
5. Le premier chalumeau pour le soudage a été conçu entre les années \_\_\_\_\_ et \_\_\_\_\_.
6. Le soudage \_\_\_\_\_ est utilisé pour souder les rails de chemin de fer
7. Le soudage automatique est très utilisé dans l'industrie \_\_\_\_\_.

Parmi les développements numériques les plus récents, citons le soudage à l'arc avancé, la réalité augmentée (RA) et la réalité virtuelle (RV), ainsi que le soudage robotisé. Une brève description de chacun d'entre eux est présentée ci-dessous.

Soudage à l'arc avancé :

- Résiste à la corrosion, ce qui le rend parfait pour les opérations de soudage chimique, nucléaire et toxique.



## Réalité augmentée (RA) et réalité virtuelle (RV) :

- La réalité augmentée rend la formation plus visuelle, plus attrayante et plus éducative. Elle permet également de réduire le coût des matériaux utilisés pour la formation, de modérer les risques et de permettre aux éducateurs de former plus de nouveaux soudeurs en même temps. La RA permet à l'utilisateur d'entrer dans un environnement réel, de toucher et de sentir un objet réel et d'« augmenter » cet objet en lui donnant une nouvelle forme, en modifiant son apparence de manière réaliste. Par exemple, grâce à la RA, un étudiant en soudage peut prendre une pièce en plastique et interagir avec elle alors qu'elle se comporte comme une pièce en acier au carbone, en acier inoxydable ou en aluminium lorsqu'elle est soudée. C'est très proche de l'expérience de soudage réelle, de sorte que les stagiaires peuvent voir et ressentir un environnement de soudage réel en utilisant un véritable équipement de soudage, tels qu'un masque de soudage et des torches de soudage.



- La RV transporte l'utilisateur dans un monde entièrement généré par ordinateur où il peut faire semblant de souder. L'expérience ressemble à celle d'un jeu vidéo.

## Soudage robotisé :

- Relie les personnes, les machines et les technologies intelligentes. Il s'agit de machines équipées de technologie numérique, y compris l'IA, utilisées aux côtés de soudeurs humains hautement qualifiés. Le soudage robotisé n'a rien à voir avec un robot humanoïde utilisant un chalumeau. Il s'agit de la nécessité de faire progresser la technologie de l'industrie 4.0. La quatrième révolution industrielle changera la façon dont la production manufacturière est automatisée grâce à l'utilisation de technologies intelligentes.



Document édité et traduit. Source : <https://seaberyat.com/en/welding-technology-trends-2021-beyond/>



## 2.

Soulignez les mots ou les phrases dans l'article portant sur les développements numériques dans le domaine du soudage pour répondre à toutes les questions ci-dessous.

*(Compétences numériques, niveau intermédiaire)*

1. Quels sont les avantages de la RA ?
2. Pourquoi le soudage à l'arc avancé est-il si utile ?
3. Que peuvent faire les apprentis soudeurs lorsqu'ils utilisent la RV ?
4. Pourquoi la RA est-elle un outil de formation si précieux ?
5. Quelle est l'incidence de la RA sur les coûts et les risques ?
6. Qu'est-ce que le soudage robotisé ?
7. Quel est l'impact attendu de la quatrième révolution industrielle sur l'industrie manufacturière ?

## MUSÉES D'OUTILS

Vous vous souvenez du Canadian Museum of Making (le musée de la Fabrication) ? Ce n'est qu'un exemple parmi d'autres des musées du monde entier consacrés à l'histoire et à l'évolution des outils utilisés dans les métiers spécialisés.

Si l'on remonte à 100, 50 ou même 10 ans en arrière, on constate que les outils utilisés par les artisans pour effectuer leur travail ont considérablement changé. Le travail qui était autrefois effectué à la main est aujourd'hui réalisé à l'aide d'outils qui utilisent des informations numériques pour vérifier leur état et accomplir les tâches. En menuiserie, on est passé de la scie à main à la scie sur table, puis à la scie qui peut être programmée pour effectuer des coupes précises des centaines de fois.

Tandis que le musée de la Fabrication s'efforce de préserver les outils du passé, le travail dans presque tous les métiers progresse à la vitesse de l'éclair, sous l'impulsion de la transformation numérique. La chronologie précédente montre l'évolution des outils utilisés dans le soudage de l'époque préhistorique à l'ère numérique, et l'article « Développements numériques dans le domaine du soudage » décrit les changements récents de manière plus détaillée.

## 3.

À l'aide des informations de la chronologie et de l'article portant sur les développements numériques dans le domaine du soudage, imaginez que vous deviez décrire l'histoire du soudage à quelqu'un. Quels sont les cinq développements les plus importants que vous choisiriez dans la chronologie ? Décrivez chaque évolution ci-dessous et expliquez pourquoi vous pensez qu'elle est si importante. Indiquez ce que vous considérez comme le plus important en tant que numéro 1.

*(Compétences numériques, niveau intermédiaire)* Les réponses peuvent varier.



1.
Raison :
2.
Raison :
3.
Raison :
4.
Raison :
5.
Raison :

**4.**

Réfléchissez maintenant à un métier qui vous intéresse et à la manière dont les outils utilisés ont pu évoluer au fil du temps. Utilisez vos compétences numériques pour rechercher des informations sur l'évolution de ce métier, depuis les premiers registres jusqu'à l'ère numérique. Visitez au moins deux sites Web différents pour compléter votre recherche. Choisissez au moins 5 faits intéressants pour compléter ce qui suit.

*(Compétences numériques, niveau intermédiaire)* Les réponses peuvent varier.



Nom du métier :

---

Sites Web visités :

1.

---

2.

---

Date de la première  
utilisation connue du  
métier :

---

Date du début de  
l'utilisation des outils  
numériques :

---

Faits intéressants :

1.

---

2.

---

3.

---

4.

---

5.

---



## SUIVRE LE RYTHME DES CHANGEMENTS

Le rythme du changement à l'ère numérique est plus rapide qu'à n'importe quel autre moment de notre histoire industrielle. Outre les compétences numériques, Mike Bocsik, l'instructeur automobile dont nous avons parlé précédemment, estime que, quelle que soit leur ancienneté, les ouvriers ont besoin d'une formation régulière et continue pour suivre les avancées technologiques — qui se produisent presque tous les trimestres dans l'industrie automobile.



« Si vous laissez les choses stagner, vous allez prendre du retard, déclare-t-il. Il est essentiel de procéder à des mises à niveau et d'aller de l'avant ».

<https://www.cbc.ca/news/canada/skilled-trades-education-1.6773564>

Une nouvelle étude de chercheurs de l'Athabasca University vient confirmer la position de Mike Bocsik : plus des trois quarts des salariés canadiens (77 %) souhaitent se recycler afin de rester au fait de l'évolution des besoins de leur travail. Les compétences numériques constituent une priorité absolue pour 70 % des personnes interrogées. <https://news.athabascau.ca/research/workplace-dynamics-study/>

Examinez ces conseils pour suivre le rythme des changements numériques.

1. Posez des questions. Les outils numériques sont comme tous les outils de travail, vous devez connaître leur fonctionnement pour pouvoir les utiliser efficacement et en toute sécurité. Si vous ne les connaissez pas, posez des questions.
2. Assurez-vous que tout logiciel que vous utilisez est toujours la version la plus récente. Téléchargez les mises à jour dès qu'elles sont disponibles ou au moins tous les six mois.
3. Veillez à ce que vos outils numériques soient sûrs, propres et sécurisés. Un café renversé est le pire ennemi de votre téléphone.
4. Assurez-vous que la manière dont vous utilisez les outils est conforme aux attentes et aux politiques de votre employeur.
5. Lisez, en ligne ou sur papier, des articles dans des revues spécialisées et des blogues pour vous tenir au courant des nouveautés.

1.

Pour chaque outil numérique figurant dans le tableau ci-dessous, indiquez si vous avez effectué les tâches identifiées et depuis combien de temps. Si vous ne possédez pas ces outils, interrogez quelqu'un qui les a en main. Notez vos réponses à l'aide des indicateurs ci-dessous, puis faites le total de vos résultats pour chaque outil.



Effectué au cours des 6 derniers mois	3 points
Effectué au cours de la dernière année	2 points
Effectué il y a plus d'un an	1 point
Jamais effectué	0 point

*(Compétences numériques, niveau intermédiaire)* Les réponses peuvent varier.

Outils numériques	TÂCHES					Totaux
	Mise à jour du logiciel	Nettoyage	Suppression de fichiers ou d'applications inutilisés	Apprentissage d'une nouvelle application ou d'un nouveau programme	Mise à jour ou installation d'un logiciel antivirus	
Téléphone portable						
Ordinateur portable ou tablette						
Ordinateur de bureau						
Autre(s) outil(s) numérique(s)						
Total des points						

Évaluez maintenant votre score total.

50—60 = Bien joué !

35—50 = Assez bien.

21 — 35 = Vous devez vraiment y travailler.

0 — 20 = Risque élevé !

Quels sont vos résultats ? Avez-vous besoin de mettre à jour vos outils numériques ?



## 2. MOTS DE PASSE ET CYBERSÉCURITÉ



Bonne Journée mondiale du mot de passe !

Bonne Journée mondiale du mot de passe !

Créée en 2013 par Intel, la Journée mondiale du mot de passe est célébrée le premier jeudi du mois de mai dans le but de sensibiliser les gens à l'importance d'une bonne hygiène des mots de passe et d'encourager les travailleurs et les particuliers à reconnaître le rôle que jouent les mots de passe forts dans la sécurisation de leur vie numérique.

Comment fêteriez-vous la Journée du mot de passe ?

Les mots de passe et la protection par mot de passe sont très importants ! De nos jours, vous avez besoin d'un mot de passe pour presque tout ce que vous faites en ligne. Qu'il s'agisse de services de diffusion en continu, de comptes de médias sociaux ou d'opérations bancaires, beaucoup d'entre nous ont des dizaines de mots de passe qu'ils utilisent tous les jours, et les pirates informatiques cherchent toujours à les deviner. Comprendre et pratiquer une excellente hygiène des mots de passe est une composante importante de la protection des mots de passe.

Un moment ! L'hygiène des mots de passe ? Vous avez entendu parler de l'hygiène de la bouche pour préserver la solidité des dents et des gencives, et de l'hygiène du lavage des mains pour limiter la propagation des virus, mais qu'est-ce que l'hygiène des mots de passe ?

En termes simples, l'hygiène des mots de passe fait référence à la manière dont vous créez des mots de passe et dont vous les gérez pour assurer la sécurité de tout ce que vous faites en ligne.

Une mauvaise hygiène en matière de mots de passe consiste à utiliser un seul mot de passe pour tout et à communiquer ce mot de passe à votre meilleur ami.

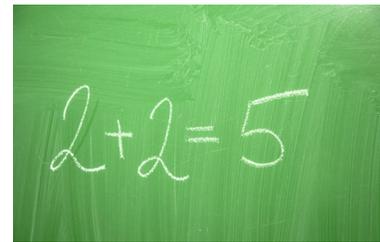
Une excellente hygiène en matière de mots de passe consiste à créer des mots de passe uniques et complexes pour chacune des activités que vous effectuez en ligne et à conserver ces mots de passe en toute sécurité.

Et comme pour la plupart des choses que vous faites en ligne, c'est VOTRE responsabilité de pratiquer une excellente hygiène en matière de mot de passe, à la maison, en classe et pour votre employeur.





Mmm. Il y a quelque chose qui cloche. Selon une enquête de LogMein, 91 % des personnes connaissent les risques liés au recyclage des mots de passe, mais seulement 58 % utilisent toujours le même mot de passe ou une variante similaire de ce mot de passe pour la plupart de leurs comptes en ligne.



1.

Avant d'en apprendre davantage sur ce que vous pouvez faire pour pratiquer une bonne hygiène en matière de mots de passe, voyons ce que vous faites déjà correctement. Complétez le questionnaire en cochant la case  $\checkmark$  à côté de chaque élément que vous faites déjà. (*Compétences numériques, niveau intermédiaire*)

N°	ITEM	$\checkmark$
1	Je change tous mes mots de passe tous les 2 ou 3 mois.	
2	J'utilise des mots de passe différents pour toutes mes applications et tous mes comptes.	
3	Je n'inclus jamais d'informations personnelles dans un mot de passe, comme le nom de ma rue.	
4	Je n'utilise jamais de lettres ou de chiffres consécutifs dans mes mots de passe.	
5	Je ne réutilise jamais mes mots de passe.	
6	Je ne communique jamais mes mots de passe.	
7	Je n'utilise jamais le nom de mon animal de compagnie comme mot de passe.	
8	Je n'utilise jamais le mot « motdepasse » comme mot de passe.	
9	Mes mots de passe comportent toujours au moins 12 caractères.	
10	Mes mots de passe contiennent toujours des lettres, des chiffres et des symboles (&, *, @).	

### Pointage

Si vous avez coché 8 à 10 cases, vous êtes un pro du mot de passe !

Si vous avez un résultat inférieur à 8, vous avez encore du travail à faire, et cette séance de formation vous y aidera.



## Qu'est-ce qu'un bon mot de passe ?

Selon « Pensez cybersécurité Canada », la plupart des gens utilisent des mots de passe qui sont « acceptables ». Cela s'explique par le fait que la plupart des applications et des comptes exigent que vous utilisiez des mots de passe contenant des lettres majuscules, des chiffres et au moins un caractère spécial.

C'est un bon début, mais vous pouvez faire mieux en suivant les conseils suivants.

1. Un mot de passe solide doit comporter au moins 12 caractères, et plus il est long, plus il est fort.
2. L'utilisation d'une combinaison complexe de caractères, de chiffres et de symboles peut vous aider à protéger vos comptes.
3. L'utilisation de toute variante de « mot de passe » pour votre mot de passe est une mauvaise idée. C'est peut-être le mot de passe le plus facile à déchiffrer, quel que soit le nombre de caractères aléatoires, de chiffres ou de variations que vous utilisez pour l'épeler (par exemple, 123m0tdep@sse765).
4. Utilisez des suites aléatoires de chiffres dans votre mot de passe, mais n'utilisez pas de chiffres (ou de lettres) qui se suivent normalement (1-2-3, M-N-O-P)
5. N'utilisez pas de séquences de chiffres personnels, comme des numéros de téléphone.
6. N'utilisez pas les noms des animaux de la famille ou d'autres informations personnelles.
7. N'utilisez pas d'informations personnelles telles que votre nom complet ou votre adresse.
8. Essayez une phrase de passe, mais mélangez l'ordre des mots.
9. Les phrases de passe doivent être un peu plus longues que les mots de passe traditionnels. Votre phrase de passe doit contenir au moins 4 mots différents et compter au moins 15 caractères.



1.

Utilisez les informations contenues dans les conseils pour identifier ce qui ne va pas avec chacun de ces mots de passe. Mettez ensuite à jour chaque mot de passe pour le rendre plus fort. (*Compétences numériques, niveau intermédiaire*)

Mot de passe	Pourquoi est-il faible ?	Réécrire pour le rendre plus fort
Abcde 3456789		
chatsattrapentsouris		
MmFd386QR990		
X31monmotdepassegh3 \$		

## Au-delà du mot de passe

De nombreux individus et organismes dépassent l'utilisation de simples mots de passe et phrases de passe en ajoutant une autre couche de protection aux connexions. La forme la plus courante de protection supplémentaire est l'authentification multifactorielle (AMF). L'AMF ajoute des étapes supplémentaires au processus de connexion qui rendent vos comptes et vos appareils plus sûrs.

L'AMF exige que vous utilisiez une combinaison de deux ou plusieurs des facteurs suivants pour accéder à vos comptes :



- *Quelque chose que vous connaissez (par exemple, un NIP (numéro d'identification personnel), un mot de passe ou une phrase de passe, des réponses à des questions de sécurité ;*
- *Quelque chose que vous avez (par exemple, une carte à puce, un jeton physique, une application d'authentification, un courriel ou un code ou toute forme de message texte envoyé d'un appareil à un autre ;*
- *Quelque chose que vous êtes (par exemple, une empreinte digitale, votre visage ou un balayage de l'iris).*

*Ajouter l'AMF à votre compte, c'est comme ajouter une alarme de maison ou de voiture qui nécessite la saisie d'un code NIP pour l'éteindre. Il s'agit d'une étape supplémentaire de protection contre les cybercriminels qui tentent de s'introduire dans le système. Même s'ils franchissent une première étape (par exemple, en devinant votre mot de passe (faible ?)), ils doivent encore franchir une deuxième, voire une troisième barrière pour accéder à votre compte ou à celui de votre employeur ou d'une autre entreprise. C'est une très bonne idée de mettre en place l'AMF pour vos comptes chaque fois que vous le pouvez. De nombreux organismes et entreprises le font couramment.*

## *Comment l'AMF fonctionne-t-elle ?*

*Après avoir saisi vos données de connexion habituelles (nom d'utilisateur et mot de passe), une ou plusieurs des choses suivantes se produiront.*

- 1. Vous recevrez un message texto, un courriel ou un message vocal contenant un mot de passe aléatoire à usage unique (ou un code) que vous devez saisir pour confirmer votre identité afin de pouvoir accéder à un service en ligne ou l'utiliser. (IMPORTANT : Si vous choisissez de recevoir un code par courriel, assurez-vous que votre compte de courriel est lui-même sécurisé. Cela signifie que vous devez activer l'AMF pour le compte de courriel électronique que vous utilisez) ;*
- 2. Vous recevrez un code par l'intermédiaire d'une application d'authentification. Il s'agit d'une application mobile qui génère un code aléatoire différent à chaque fois que vous vous connectez. Elle est plus sûre que la réception d'un code par texto. Pour utiliser une application d'authentification, vous devez d'abord la télécharger sur votre appareil ;*
- 3. Vous devez utiliser l'une de vos caractéristiques uniques pour authentifier votre identité. Il peut s'agir de fournir l'un des cinq types d'identifiants biométriques les plus courants : empreintes digitales, reconnaissance faciale, voix, balayage de l'iris ou schéma des veines de la paume ou du doigt pour accéder à votre appareil ou à vos applications mobiles. L'utilisation de la biométrie dans le cadre de l'AMF est pratique, car vous ne pouvez pas égarer une partie de vous-même !*



1.

Écrivez la signification de chacune des abréviations ou chacun des mots suivants.  
(*Compétences numériques, niveau de base*)

ABRÉVIATION ou MOT	SIGNIFICATION
NIP	
TEXTO	
AMF	
CODE	

2.

L'authentification à plusieurs facteurs exige que vous établissiez un lien entre qui vous êtes, quelque chose que vous connaissez et quelque chose que vous possédez afin de fournir une couche supplémentaire de sécurité numérique.

Identifiez chaque facteur énuméré ci-dessous comme étant soit :

1. Qui vous êtes.
2. Ce que vous savez.
3. Ce que vous avez.

(*Compétences numériques, niveau intermédiaire*)

FACTEUR	N°
NIP	
Lecteur d'empreintes digitales	
Jeton matériel	
Carte à puce	
Questions de sécurité	
Reconnaissance vocale	
Texto	
Numériseur d'iris	
Authentificateurs basés sur des applications	
Reconnaissance faciale	
Mots de passe et phrases de passe	



### 3.

Quand avez-vous eu besoin d'utiliser l'AMF ? Pour des opérations bancaires ? Pour le magasinage ? Au travail ? D'autres situations ? Citez jusqu'à trois de ces situations et décrivez les mesures que vous avez dû prendre pour chacune d'entre elles. Vous n'avez pas encore utilisé l'AMF ? Interrogez quelqu'un qui l'a fait.

*(Compétences numériques, niveau intermédiaire)*

Situation : \_\_\_\_\_

Étapes :

Situation : \_\_\_\_\_

Étapes :

Situation : \_\_\_\_\_

Étapes :

### La protection à l'aide d'un mot de passe est-elle vraiment si importante ?

Oui, elle l'est. C'est une affaire importante pour vous et pour tout employeur pour lequel vous travaillez.

Les cybercriminels ne se contentent pas de cibler les grandes entreprises et les organismes pour accéder à leurs systèmes de données, obtenir des informations sensibles et exiger des rançons. Les petites entreprises sont devenues des cibles tout aussi importantes, sinon plus, pour les pirates informatiques. En fait, 71 % des petites et moyennes entreprises (PME) ont déclaré avoir subi au moins une cyberattaque, selon l'Autorité canadienne pour les enregistrements Internet (ACEI). Et cette petite ou moyenne entreprise, c'est peut-être celle pour laquelle vous travaillez. Parfois, cela se produit parce qu'une PME sous-traite des travaux à une entreprise plus importante. Voici un exemple concret.

En 2020, une entreprise de construction canadienne qui a décroché des contrats d'une valeur de plusieurs millions de dollars avec l'armée et d'autres ministères fédéraux a été victime d'une attaque par rançongiciel. Les attaques par rançongiciel consistent à pirater le système d'une entreprise — souvent à l'aide d'un mot de passe faible ou d'une



escroquerie par hameçonnage — pour installer un logiciel malveillant qui endommage le système informatique de l'entreprise, puis à exiger un paiement en espèces pour réparer les dégâts. Dans cette attaque, les pirates ont volé 60 Go de données.

L'entreprise ayant remporté près de 50 contrats fédéraux entre 2006 et 2015, d'une valeur totale de plus de 400 millions de dollars, la GRC a été fortement impliquée dans l'enquête. Commentant l'enquête, le président de l'Association canadienne des industries de défense et de sécurité a déclaré : « Lorsque nous examinons les principaux cas de piratage qui se sont produits, en particulier dans le domaine de la défense, où l'on connaît le vol d'informations sur les avions de combat, ces informations n'ont pas été volées chez l'entrepreneur principal, elles ont été volées dans un tout petit magasin fournissant des widgets ». <https://www.cbc.ca/news/politics/ransomware-bird-construction-military-1.5434308>

En réalité, même si vous travaillez dans une petite entreprise de fabrication de widgets, votre erreur peut conduire à une attaque beaucoup plus importante. Les études montrent que les petites entreprises sont plus vulnérables aux cyberattaques parce qu'elles ne possèdent généralement pas les ressources de sécurité et la formation à la cybercriminalité pour les employés dont disposent les grandes entreprises, de sorte qu'elles sont moins en mesure de se protéger contre la cybercriminalité.

Les employeurs pour lesquels vous travaillez auront mis en place des politiques et des procédures pour assurer la sécurité des données de leur entreprise et vous devrez les respecter à la lettre. Si vous ne le faites pas, vous risquez d'être renvoyé.

L'un des meilleurs moyens pour les employeurs de préserver la sécurité de leurs informations en ligne est d'exiger de leurs employés qu'ils suivent régulièrement une formation en matière de cybersécurité. Vous trouverez ci-dessous un aperçu des éléments communs des programmes de formation des employés dans ce domaine.

Qu'est-ce qui est généralement inclus ?

- La gestion des mots de passe
- La sécurisation des courriels
- La sécurisation de votre équipement
- Les pratiques et les attentes en matière de cybersécurité propres à l'entreprise.

Quand suivre la formation ?

- Lors de l'embauche
- Ensuite, tous les quelques mois

Comment la formation est-elle offerte ?

- En ligne ou en personne ou une combinaison des deux
- Dans le cadre de vos heures de travail habituelles



1.

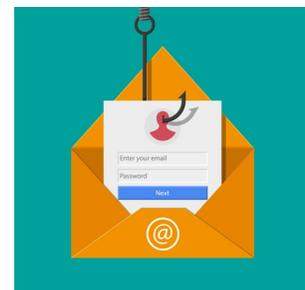
Dans le scénario qui suit, Martin travaille depuis longtemps dans l'industrie manufacturière, mais il est un nouvel employé de DIGICAN, une entreprise manufacturière qui pratique un niveau élevé de sécurité numérique. C'est nouveau pour Martin et il a déjà du mal à accepter certaines pratiques. Martin rejette la faute sur la technologie et affirme que c'est le problème de l'employeur et non sa responsabilité. Lisez ce qui s'est passé lors de son premier jour et soulevez tout ce que vous pensez qu'il aurait pu faire différemment. *(Compétences numériques, niveau intermédiaire)*

Le premier jour, Martin était impatient de connaître l'entreprise et il est arrivé en retard à la séance d'information sur la sécurité. Le temps qu'il arrive, le formateur avait une autre réunion et il a donc donné à Martin des instructions écrites et reporté la formation à trois jours plus tard. Martin a suivi les instructions pour se connecter au système de l'entreprise. Il a créé un mot de passe (Martin123456) et l'a immédiatement noté pour ne pas l'oublier. Il l'a écrit sur un post-it qu'il a collé sur son poste de travail. Les instructions indiquent ensuite qu'il faut créer un profil RH en ligne. Martin a réutilisé le même mot de passe pour ne pas l'oublier. Pendant qu'il créait son profil, Martin a vu qu'il y avait un nouveau courriel dont l'objet était FÉLICITATIONS. Il n'a pas reconnu la personne qui l'avait envoyé, mais c'était normal, car il était nouveau et ne connaissait personne. Il a supposé qu'il s'agissait d'un message de bienvenue et a cliqué sur un lien inclus dans le message, ce qui a fait virer son écran au rouge et a verrouillé l'ordinateur. Martin a éteint son ordinateur, n'a rien dit à personne et est allé voir s'il pouvait obtenir son équipement de protection individuelle (ÉPI).

## Sécurité des messages

La sécurité des messages est l'un des sujets les plus importants en matière de cybersécurité pour les employés. Les auteurs d'attaques par message n'ont pas besoin de savoir comment déchiffrer votre mot de passe. Lorsque vous répondez à une attaque par courriel ou par message texto, vous ouvrez la porte au pirate.

Un grand nombre de cyberattaques sont lancées au moyen de techniques de messagerie connues sous le nom d'hameçonnage (phishing), ou de techniques connexes connues sous les noms de saumurage (smishing), harponnage (spear phishing) et chasse à la baleine (whaling). Les cybercriminels utilisent ces types de messages pour tenter de voler des informations sensibles à des personnes en se faisant passer pour des expéditeurs légitimes tels que la banque de la personne ou un collègue. L'un des moyens les plus courants pour envoyer une attaque est le courriel.





## NE MORDEZ PAS À L'HAMEÇON !

**Hameçonnage (phishing) :** tout message qui a été délibérément falsifié pour faire croire qu'il provient d'un expéditeur authentique.

**Saumurage (smishing) :** tout message d'hameçonnage envoyé par texto (également connu sous le nom de message textuel).

**Harponnage (spear phishing) :** des messages sur mesure envoyés à une personne ou à un petit groupe de personnes, ce qui en fait une approche beaucoup plus ciblée.

**Chasse à baleine (whaling) :** le harponnage (spear phishing) visant des cadres supérieurs ou des victimes importantes.

Comme tous les aspects de la cybersécurité, reconnaître et prévenir les attaques de type hameçonnage est une responsabilité partagée. Les employeurs ont la responsabilité de former leurs employés à la détection et à la lutte contre l'hameçonnage. Les employés sont responsables de la mise en œuvre de cette formation.

Il existe des indices qui permettent de penser qu'un courriel peut être une attaque d'hameçonnage.

1. Les attaques par hameçonnage utilisent souvent un langage urgent ou menaçant. Méfiez-vous des messages qui vous pressent de répondre rapidement, surtout si la demande est bizarre.
2. Pièces jointes et liens suspects. Soyez attentif aux liens dont l'URL n'est pas familière et aux pièces jointes dont le nom ou le type de fichier (comme un .exe) est étrange et que vous n'avez pas demandé, en particulier si elles proviennent d'un expéditeur suspect. Ne cliquez pas dessus.
3. Adresses courriel d'expéditeurs étranges. Un message peut provenir d'une banque, mais lorsque vous survolez le courriel du « service comptabilité », l'adresse de l'expéditeur est en fait la suivante « [max@cx3bancor.com](mailto:max@cx3bancor.com) »
4. Demandes d'informations sensibles ou personnelles. Méfiez-vous des liens qui vous dirigent vers des pages de connexion et des demandes concernant vos informations personnelles (par exemple, quelqu'un qui vous demande le mot de passe de votre compte).
5. Fautes de frappe et mauvaise conception. Soyez attentif aux adresses électroniques incorrectes, aux liens suspects et à toute faute d'orthographe ou de grammaire inhabituelle, ainsi qu'aux logos imprécis ou flous, ou aux courriels d'entreprise présentant des problèmes de mise en forme.

Si vous cliquez sur un message qui s'avère être une attaque par hameçonnage, rappelez-vous :

- Ne paniquez pas !
- Ne faites pas comme si de rien n'était !
- N'éteignez pas votre ordinateur !
- Ne transmettez pas le message à un autre membre de votre organisme (y compris au service informatique !).



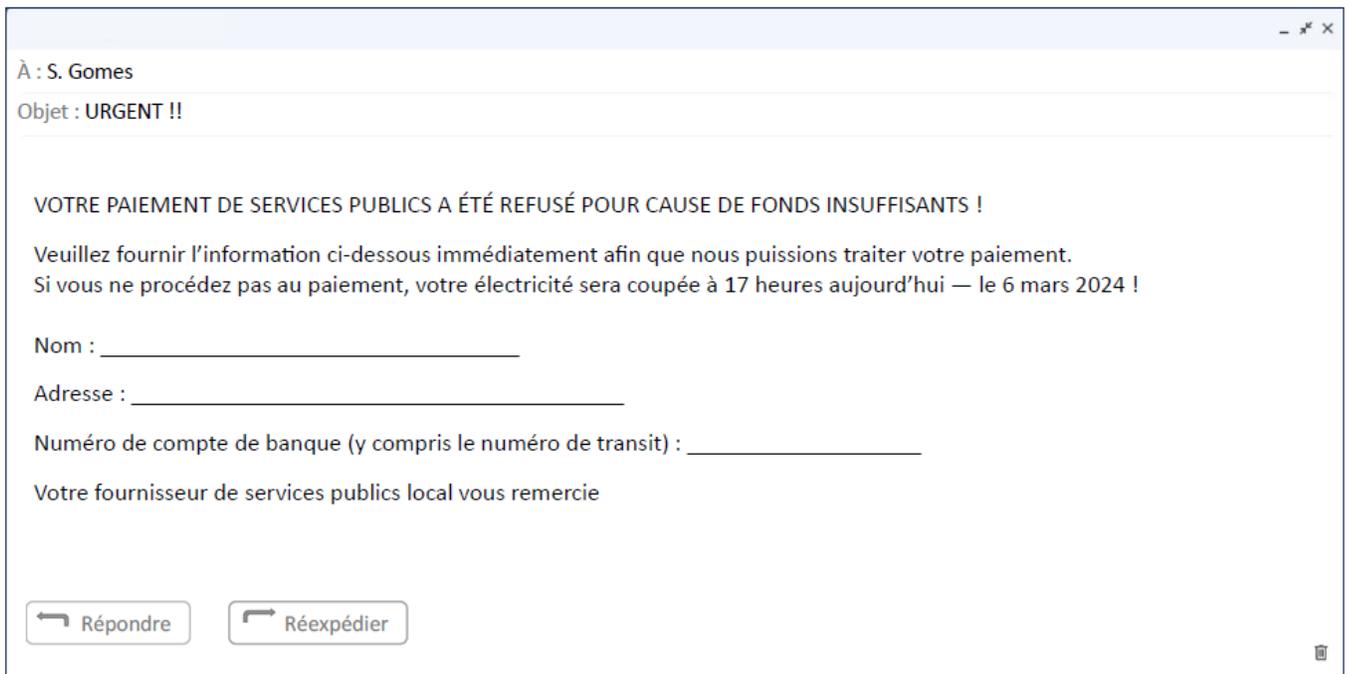
Vous pouvez prendre certaines mesures importantes :

- Contactez immédiatement votre service informatique ou votre superviseur et faites-leur connaître ce qui s'est passé.
- Votre service informatique vous demandera probablement de :
  - Changer votre mot de passe.
  - Activer l'AMF si possible.
  - De suivre une formation plus poussée en matière de sécurité afin d'éviter que cela ne se reproduise.

1.

Dans chacun des courriels de la page suivante, surlignez trois indices indiquant qu'il pourrait s'agir d'une attaque par hameçonnage.

(*Compétences numériques, niveau intermédiaire*)



À : S. Gomes

Objet : URGENT !!

VOTRE PAIEMENT DE SERVICES PUBLICS A ÉTÉ REFUSÉ POUR CAUSE DE FONDS INSUFFISANTS !

Veillez fournir l'information ci-dessous immédiatement afin que nous puissions traiter votre paiement.  
Si vous ne procédez pas au paiement, votre électricité sera coupée à 17 heures aujourd'hui — le 6 mars 2024 !

Nom : \_\_\_\_\_

Adresse : \_\_\_\_\_

Numéro de compte de banque (y compris le numéro de transit) : \_\_\_\_\_

Votre fournisseur de services publics local vous remercie



À : C. Fredericks

Objet : PROBLÈME DE MOT DE PASSE !!

**MOT DE PASSE EXPIRÉ !!**

Votre mot de passe pour votre compte MS Outlook est expiré !

Afin d'assurer la sécurité de votre compte, votre mot de passe cessera de fonctionner dans une heure.

Vous devez modifier votre mot de passe immédiatement !

Cliquez sur le lien ci-dessous pour modifier votre mot de passe

<http://msoutlooks.service.com/wolskie/reset>

**Il s'agit uniquement d'une notification du système.  
Ne pas répondre.**



## 3. GÉRER LES MÉDIAS SOCIAUX AVEC INTELLIGENCE

Les médias sociaux comprennent toute plateforme en ligne que vous utilisez pour produire et partager des données afin de créer ou d'étendre vos réseaux sociaux. Vous pensez que les médias sociaux ne servent qu'à vous amuser ? C'EST FAUX ! Les médias sociaux sont également un outil important pour obtenir et conserver un emploi. Ce que vous publiez sur les médias sociaux peut amener un employeur potentiel ou un organisme bénévole à déterminer que vous correspondez parfaitement aux besoins de son entreprise, à sa formation en apprentissage ou à l'occasion qui s'offre à lui, ou qu'il ne veut absolument pas travailler avec vous. Tout dépend de vous.



*Vous êtes responsable du contenu de vos informations en ligne.*

*Vous êtes aussi responsable de la confidentialité et de la sécurité de vos informations en ligne.*

*Vous pensez que ces responsabilités ne sont pas importantes ? Vous pensez tout connaître des médias sociaux parce que vous les utilisez depuis toujours ? C'est ce qu'a fait un joueur de football universitaire lors de ce qui aurait dû être la meilleure soirée de sa carrière. Faites la lecture de l'histoire ci-dessous.*

Le trophée Heisman est décerné chaque année au meilleur joueur de football universitaire des États-Unis. En 2018, le soir même de sa remise, les médias ont fait état de plusieurs gazouillis (tweet) négatifs que le champion avait écrits des années auparavant, alors qu'il était encore à l'école secondaire. Sur Twitter (X), le joueur a utilisé des insultes homophobes pour parler de ses amis. Il s'est excusé à plusieurs reprises et a déclaré qu'il s'agissait d'une blague, mais les médias du monde entier ont relayé l'histoire et sa réputation a été compromise. Bien que les gazouillis originaux aient finalement été supprimés, il est toujours possible de rechercher et de lire l'histoire en ligne.

*Et avant de penser que seuls les jeunes commettent des erreurs dans les médias sociaux, faites la lecture de ce qui suit.*

Un sous-traitant de Chrysler Automobiles a posté un gazouillis obscène sur le compte officiel de la marque Chrysler. Son message sur Twitter (X) se lit comme suit : « Je trouve ironique que Détroit soit connue comme la #motorcity et pourtant, personne ici ne sait conduire (juron) ». Il avait



l'intention d'afficher ce commentaire sur son compte personnel, mais il l'a placé par erreur sur le fil du compte de la marque Chrysler alors qu'il était coincé dans un embouteillage sur l'autoroute. Il a perdu son emploi, et son gazouillis est l'une des raisons pour lesquelles Chrysler n'a pas renouvelé son contrat avec son (ancien) employeur. « En tant que citoyen de Détroit, c'était sympa de savoir que le travail que je faisais chez Chrysler contribuait à cette grande reprise d'activités pour Détroit et les trois principales compagnies automobiles, a-t-il déclaré au Detroit Free Press. J'y avais mis tout mon cœur et toute mon âme. C'est dommage que tout mon travail soit effacé par 140 caractères ».

1. Utilisez les informations tirées des deux situations pour compléter le tableau.  
(Compétences digitales, niveau intermédiaire)

	Joueur de football	Entrepreneur chez Chrysler
Quelle plateforme de médias sociaux ont-ils utilisée ?		
Quel type de média ont-ils publié (vidéo, commentaire, etc.) ?		
Pourquoi la publication était-elle inacceptable ?		
Qu'est-il arrivé à la personne qui a publié le message ?		
Qu'aurait pu faire chaque personne qui a publié un gazouillis pour éviter le problème ?		
Pensez-vous que la réaction au gazouillis du joueur de football était juste ? Pourquoi ou pourquoi pas ?		
Pensez-vous que la réaction au gazouillis de l'entrepreneur était juste ? Pourquoi ou pourquoi pas ?		



Que vous pensiez que les réactions et les punitions étaient justes ou non est intéressant, toujours est-il qu'elles se sont produites. La bonne nouvelle, c'est qu'il y a des choses que vous pouvez faire pour éviter de commettre ce genre d'erreurs et donner une image positive de votre identité en ligne.

Commençons par la manière dont vous utilisez les médias sociaux.

## 2.

Passez en revue la liste des plateformes en ligne populaires ci-dessous et mettez un ✓ à côté de chacune de celles que vous utilisez. Utilisez les lignes vides pour en ajouter d'autres si elles ne trouvent pas dans la liste. Remplissez ensuite les colonnes restantes pour les plateformes que vous avez sélectionnées.

*(Compétences numériques, niveau de base)*

Plateforme	✓ si vous l'utilisez	Nombre de fois par semaine que vous affichez quelque chose	Nombre de fois par semaine que vous affichez un commentaire ou partagez l'information de quelqu'un d'autre
Facebook			
Instagram			
Twitter/X			
YouTube			
LinkedIn			
Snapchat			
TikTok			
Total de publications, de commentaires et de messages partagés par semaine			



Total des publications, de commentaires et de messages partagés par année		
Nombre total de pièces d'information partagées entre la 8e année et l'obtention de son diplôme		

Même si vous ne publiez qu'une fois par jour, cela représente 365 messages par an, soit 1 825 informations entre la huitième année et la fin des études secondaires. Cela fait beaucoup d'informations sur toi, sur ce que tu penses, sur ce que tu aimes ou n'aimes pas, qui circulent sur Internet.

Les choses qui sont publiées sur Internet peuvent y rester pour toujours. Même si vous effacez quelque chose, si quelqu'un d'autre l'a déjà partagé, cette information est toujours là. Il est très important de contrôler qui peut voir vos messages avant que vous ne décidiez de les publier. C'est là où les paramètres de confidentialité entrent en jeu.



Les plateformes de médias sociaux (applications et pages Web) sont dotées de paramètres de confidentialité gratuits qui permettent aux utilisateurs de contrôler les personnes qui peuvent consulter les informations qu'ils publient.

Les paramètres de confidentialité les plus élémentaires sont public et privé.  
1. Public signifie que toute personne ayant accès à la plateforme peut voir vos messages.

2. Privé signifie qu'un groupe limité de personnes, par exemple les personnes que vous avez identifiées comme « amis », peut consulter vos informations.

Il est conseillé de revoir régulièrement vos paramètres de confidentialité. Déterminez comment ajuster les paramètres selon les applications et les publics, en fonction de ce que vous publiez.

Même si vous publiez quelque chose que vous pourriez regretter, en contrôlant vos paramètres de confidentialité, vous pouvez au moins limiter le nombre de personnes qui le verront. Cela signifie aussi que vous pouvez limiter les informations auxquelles les étrangers ont accès et réduire ainsi les risques de piratage et de vol d'informations personnelles.

Mais il est important de se rappeler que si les paramètres de confidentialité permettent de protéger votre identité en ligne dans la plupart des cas, ils ne sont pas infaillibles. Un pirate informatique déterminé peut toujours accéder à des informations que vous avez partagées en ligne et que vous souhaitez garder confidentielles entre amis.



Le Commissariat à la protection de la vie privée du Canada (CPVP) a publié des conseils pour les Canadiennes et Canadiens sur la façon de configurer et d'ajuster les paramètres de confidentialité.

Voici quelques conseils utiles :

- Avant de cliquer automatiquement sur « accepter », faites la lecture des politiques de confidentialité pour apprendre quelles informations personnelles sont collectées et quels sont les contrôles de confidentialité disponibles. Si vous n'êtes pas à l'aise, ne vous abonnez pas.
- Examinez les paramètres par défaut d'une application et ajustez-les si nécessaire.
- Recherchez les options permettant de désactiver les paramètres de géolocalisation ou de limiter le suivi à la seule période où vous utilisez le service.
- Ne vous connectez pas automatiquement à une application à partir d'une autre. Créez une nouvelle identité.
- Ne partagez pas d'informations personnelles telles que votre numéro de téléphone.
- Recherchez des options qui vous permettent de supprimer régulièrement votre historique.
- Ne considérez pas la révision de vos paramètres comme quelque chose que vous faites une fois pour ensuite oublier. De nombreux sites modifient régulièrement les options de leurs paramètres. Il est également utile de revenir en arrière pour évaluer vos paramètres et vous assurer que vous êtes toujours à l'aise avec vos décisions antérieures.

1.

Deux des choses les plus importantes que vous puissiez faire pour protéger votre identité sont de comprendre comment fonctionne la protection de la confidentialité en ligne et de vérifier régulièrement vos paramètres.

Indiquez si chaque affirmation ci-dessous est vraie ou fausse. Si l'affirmation est fausse, réécrivez-la pour qu'elle soit vraie (la première est déjà faite pour vous).

*(Compétences numériques, niveau intermédiaire)*

Les paramètres de confidentialité assurent une protection totale. VRAI FAUX

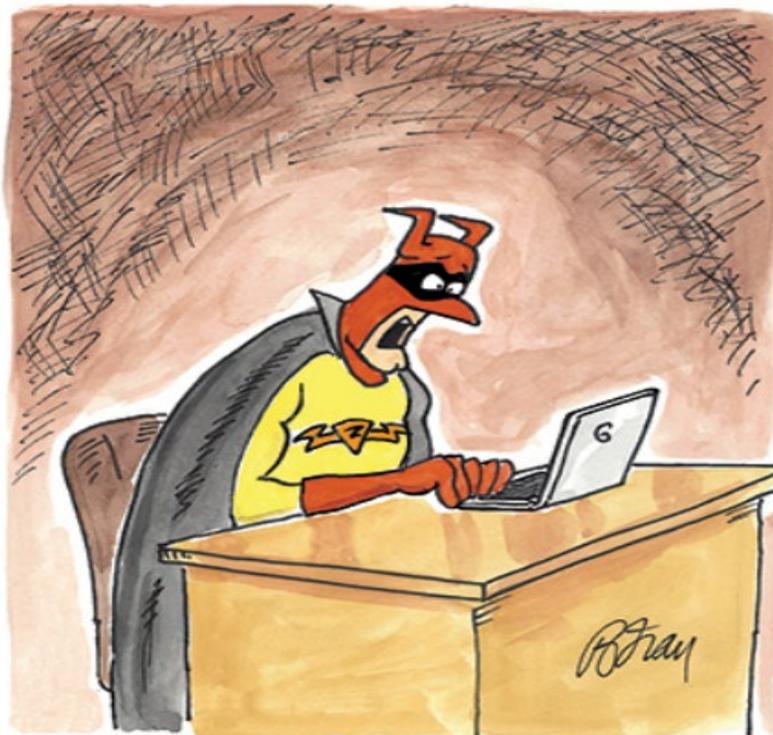
*Les paramètres de confidentialité n'offrent pas une protection Totale.*

Partager des informations personnelles en ligne, comme votre adresse, est sans danger. VRAI FAUX

Les paramètres de confidentialité peuvent être modifiés. VRAI FAUX



Les paramètres de confidentialité sont un bon moyen de protéger la confidentialité des informations. VRAI FAUX
Public signifie que tout le monde sur le site d'un média social peut voir ce que vous publiez. VRAI FAUX
Se connecter à une application à partir d'une autre est rapide et sûr. VRAI FAUX
Une fois que vous avez lu une politique de confidentialité, vous n'avez plus besoin de lire les mises à jour. VRAI FAUX
Les paramètres de confidentialité coutent plus cher. VRAI FAUX



« ZUT! ILS VOLENT D'ABORD MA VÉRITABLE IDENTITÉ, PUIS MON IDENTITÉ SECRÈTE ! »

" DANG, FIRST THEY STEAL MY IDENTITY, THEN THEY STEAL MY SECRET IDENTITY! "

<https://www.priv.gc.ca/en/about-the-opc/publications/illustrations/>



Maintenant que vous connaissez les raisons pour lesquelles les paramètres de confidentialité sont importants pour protéger votre identité en ligne, vérifions si vous les utilisez bien et si vous pouvez améliorer certains aspects.

- 1.** Remplissez le document d'autocontrôle en mettant un ✓ dans la boîte qui décrit le mieux la fréquence à laquelle vous effectuez chaque tâche. Ajoutez ensuite les ✓ dans chaque colonne.  
(*Compétences numériques, niveau intermédiaire*) Les réponses peuvent varier.

### Autocontrôle de la protection de la confidentialité

À quelle fréquence faites-vous les choses suivantes ?	En fonction d'un horaire fixe	Quand j'y pense	Jamais
Revoir vos paramètres de confidentialité actuels			
Vérifier qui peut voir vos publications			
Réviser vos profils			
Mettre à jour votre liste d'amis			
Limiter la connexion à partir d'applications de tierce partie			
Ajouter un rappel de calendrier pour vous rappeler de revoir vos paramètres			
Lire la politique de confidentialité, y compris les mises à jour, de toutes les applications que vous utilisez			
TOTAUX			

Tous les crochets devraient figurer dans la première colonne si vous êtes bien protégé. Quels sont vos résultats ? Que pouvez-vous améliorer ?



Pour empêcher vos employeurs ou d'autres personnes de consulter des contenus que vous ne voulez pas qu'ils voient, vous pouvez décider de tout rendre privé, ou même de ne pas avoir d'identité en ligne du tout.



Malheureusement, d'après les études, c'est une mauvaise idée, car ne pas avoir de présence numérique peut rendre certains organismes méfiants et limiter les possibilités d'accès à des postes qui vous pourraient vous intéresser. Ainsi, vous pouvez publier, mais publiez de manière intelligente.

L'une des choses les plus rapides que vous puissiez faire pour vérifier votre identité en ligne est de faire une recherche sur Google à votre sujet régulièrement. La recherche de votre propre nom vous montrera ce que les autres voient lorsqu'ils font la même chose. Selon les experts, il est conseillé de faire une telle recherche au moins trois fois par an. Lorsque vous effectuez une recherche sur votre nom, vous devez vous attendre à voir apparaître des images et des messages que vous vous rappelez avoir publiés, mais vous serez peut-être surpris de voir surgir d'autres choses que vous n'avez pas publiées.

## Recherche



1.

Suivez les étapes suivantes pour effectuer une recherche à votre sujet sur Google et répondez aux questions

(*Compétences numériques, niveau intermédiaire*). Les réponses peuvent varier.

Inscrivez tout simplement votre nom dans la barre de recherche de Google. Combien de résultats avez-vous trouvés ?

Inscrivez maintenant votre nom entre guillemets et la ville où vous habitez. Combien de résultats, cette fois-ci ?

2.

Pour répondre aux questions suivantes, cherchez au moins dans les 3 premières pages de résultats.

(*Compétences numériques, niveau intermédiaire*) Les réponses peuvent varier.

Quelle est une publication que vous avez trouvée et que vous vous souvenez d'avoir publiée ?



Quelle est une publication que vous avez trouvée et dont vous ne connaissiez pas l'existence ?

En regardant tous les résultats, indiquez 5 mots qui, selon vous, vous décrivent, selon cette recherche.

En regardant tous les résultats, y a-t-il quelque chose que vous préféreriez ne pas voir ?

Saviez-vous que les résultats de Google sont personnalisés pour chaque utilisateur ? C'est vrai. Alors maintenant que vous avez terminé l'activité, c'est une bonne idée de demander à quelqu'un d'autre de vous chercher sur Google pour voir ce qu'il trouve qui n'a peut-être pas été inclus dans les résultats de votre recherche.

### Qu'est-ce que vos médias sociaux disent de vous ?

Bien que certaines provinces et certains territoires disposent de lois interdisant aux employeurs d'utiliser les vérifications d'antécédents numériques lors de l'embauche, beaucoup le font encore, et ils peuvent librement utiliser les vérifications numériques pour décider de promouvoir ou de congédier des employés après qu'ils ont été embauchés.

Des vérifications numériques des antécédents sont également effectuées pour décider d'admettre un apprenti ou un étudiant dans un établissement d'enseignement postsecondaire, ainsi que dans certains organismes de bénévolat. De nombreux établissements d'enseignement postsecondaire utilisent les médias sociaux pour identifier les étudiants qui semblent savoir comment concilier de manière responsable le plaisir et le travail scolaire. Les organisateurs de bénévolat recherchent des personnes qui sont aussi passionnées qu'eux et qui savent comment partager leurs passions et leur vie en ligne de façon respectueuse.

Selon un article paru en 2023 dans le Times Colonist, journal de la Colombie-Britannique :

Les établissements postsecondaires au Canada ont tous leurs propres critères d'admission. La *University of British Columbia*, par exemple, n'évalue pas le comportement des candidats potentiels sur les médias sociaux. On indique que si un nouvel étudiant devait publier un contenu inapproprié sur un site de médias sociaux administré par l'université, celle-ci réagirait « au cas par cas » et se réserverait le droit de refuser l'admission.

L'université conseille aux futurs étudiants de se comporter en ligne en partant du principe que tout message, même privé, peut être utilisé contre eux.



Les candidats à l'admission à l'université doivent également garder à l'esprit que les offres d'admission peuvent toujours être révoquées. « Tout ce que vous partagez peut affecter votre réputation et des décisions importantes dans votre vie », a déclaré un porte-parole de l'UBC. « Cela reste un véritable facteur d'incertitude dans le processus d'admission ».

1.

Que signifie exactement cette politique ? Pour vous assurer que vous comprenez ce qu'ils disent, associez les synonymes aux mots de l'article.  
(*Compétences numériques, niveau intermédiaire*)

TIRÉ DE L'ARTICLE	SYNONYME
Facteur d'incertitude	
Établissement postsecondaire	
Au cas par cas	
Évaluer	
Critères	

### SYNONYMES

Individuellement  
Standards  
Quelque chose difficile à prédire  
Juger  
Collèges et universités

2.

Complétez chaque phrase par « fait » ou « ne fait pas » pour la rendre vraie.  
(*Compétences numériques, niveau intermédiaire*)

L'université \_\_\_\_\_ la vérification des médias sociaux de ses candidats.

L'université \_\_\_\_\_ la vérification des médias sociaux des étudiants inscrits.

L'université \_\_\_\_\_ en sorte que les étudiants sont responsables de ce qu'ils affichent en ligne.

L'université \_\_\_\_\_ en sorte que l'on traite chaque cas de la même façon.



- 3.** Pensez maintenant à vos propres médias sociaux. Imaginez que vous inscrivez à une formation, désirez obtenir un nouvel emploi ou demandez une promotion. Quelle impression voudriez-vous que la personne qui vous interroge retienne de votre identité en ligne ? Notez vos idées dans l'espace ci-dessous.

*(Compétences numériques, niveau intermédiaire)*

---

---

- 4.** Choisissez l'un des comptes de médias sociaux que vous utilisez le plus souvent. Utilisez les idées que vous avez notées comme critères pour passer en revue au moins quatre messages que vous avez publiés récemment. Décidez si vous devez laisser le message affiché ou le supprimer. Il peut s'agir d'un commentaire, d'une photo ou d'un lien : tout ce qui vient clairement de vous. N'oubliez pas de vérifier non seulement votre message original, mais aussi ce qu'il est devenu depuis. Quels sont les commentaires ou les liens qui sont maintenant associés au message ? Êtes-vous à l'aise avec ceux-ci ? Répondent-ils aux critères que vous avez identifiés ? Notez vos résultats dans le tableau ci-dessous.

*(Compétences numériques, niveau intermédiaire)*

Publication 1

---

Décision :

---

Raison :

---

Publication 2

---

Décision :

---

Raison :

---



---

## Publication 3

---

Décision :

---

Raison :

---

## Publication 4

---

Décision :

---

Raison :

---

La bonne nouvelle, c'est que vous pouvez également utiliser les médias sociaux non seulement pour vous présenter comme vous voulez être vu, mais aussi pour identifier les employeurs et les débouchés pour lesquels vous aimeriez être pris en considération.

Même les petites entreprises utilisent les médias sociaux pour permettre à leurs clients potentiels d'en savoir plus sur elles et sur les services qu'elles fournissent. Certaines entreprises utilisent leurs canaux de médias sociaux pour expliquer ce que c'est que de travailler chez elles. Cela leur permet d'attirer les personnes qui leur conviennent le mieux et peut vous aider à déterminer si l'entreprise vous convient.

Il est particulièrement important d'effectuer des recherches sur les médias sociaux lorsque vous cherchez activement un emploi ou que vous essayez d'en savoir plus sur le secteur dans lequel vous aimeriez travailler.

1. Choisissez une entreprise pour laquelle vous pensez que vous aimeriez travailler et qui possède au moins un compte de médias sociaux actif lié à son site Web. Les comptes les plus populaires sont Instagram et Facebook. Identifiez l'entreprise, puis répondez à des questions concernant trois de ses publications.  
(*Compétences numériques, niveau intermédiaire*)



Nom de l'entreprise	
Site Web	
Type de compte de média social	
<i>Publication 1</i> Quel est le sujet ?	
Qu'est-ce que cette publication vous suggère à propos de l'entreprise ?	
Pensez-vous que vous pourriez y travailler ?	
<i>Publication 2</i> Quel est le sujet ?	
Qu'est-ce que cette publication vous suggère à propos de l'entreprise ?	
Pensez-vous que vous pourriez y travailler ?	
<i>Publication 3</i> Quel est le sujet ?	
Qu'est-ce que cette publication vous suggère à propos de l'entreprise ?	
Pensez-vous que vous pourriez y travailler ?	





## 4. QUESTIONS D'ARGENT EN LIGNE

### LE COUT DE LA COMMODITÉ

Il ne fait aucun doute que la possibilité de transférer de l'argent en ligne facilite la vie. Les chèques de paie sont automatiquement déposés dans les comptes bancaires personnels. Les factures sont automatiquement payées à la date prévue, de sorte qu'il n'y a jamais de paiement manqué ou de frais d'intérêt. Et le fait de pouvoir appuyer sur « payer maintenant », bien installé dans son fauteuil préféré signifie qu'il suffit d'un clic pour commander presque tout ce que l'on veut.

Bien entendu, cette rapidité et cette commodité ont un prix. Parfois, il s'agit d'une somme d'argent, parfois d'une perte de données personnelles tout aussi précieuses.

Mais bon, vous êtes un « enfant du numérique ». Vous cliquez et envoyez des textos presque depuis que vous savez marcher. Personne ne vous trompera en ligne, n'est-ce pas ?

Malheureusement, ce n'est pas le cas. En fait, les recherches confirment que les jeunes sont les plus susceptibles d'être victimes de fraude en ligne.



- Au Canada, les Canadiens plus âgés (55+) sont parmi les moins susceptibles de déclarer être conscients d'avoir été victime d'une fraude ou d'une arnaque à un moment ou à un autre de leur vie (31 % contre 50 % pour les 18-54 ans). En comparaison, près des deux tiers (63 %) des Canadiens plus jeunes (18-34 ans) admettent être conscients d'avoir été victimes de fraude ou d'arnaque à un moment ou à un autre. (IPSOS 2023)
- Aux États-Unis, en 2022, les moins de 20 ans ont perdu 101,4 millions de dollars à cause d'arnaques en ligne, selon une étude récente de la nouvelle compagnie de cybersécurité Social Catfish, qui a cité les chiffres du rapport sur la criminalité sur Internet du *Federal Bureau of Investigation*. (CNBC 2023)
- Au Royaume-Uni, les personnes âgées de 16 à 34 ans sont beaucoup plus susceptibles d'être victimes d'arnaque et représentent plus de la moitié des arnaques subies au Royaume-Uni. (local.gov.uk 2023)

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ipsos.com/sites/default/files/ct/news/documents/2023-02/CPA%20Fraud%20Survey%20Factum%202023\_1.pdf



La bonne nouvelle, c'est que, comme pour tout ce que vous faites en ligne, il existe des mesures que vous pouvez prendre pour protéger vos transactions et reconnaître les fraudeurs qui tentent de profiter de vous. Alors, commençons !

## FRAUDES ET ARNAQUES

Les fraudes et les arnaques sont les moyens les plus courants de tromper les gens en ligne. De nombreuses personnes utilisent les mots fraudes et arnaques de manière interchangeable ; bien que leurs significations soient semblables, ce n'est pas exactement la même chose.

La fraude implique que quelqu'un (un pirate informatique) vole vos informations (généralement financières) telles que les numéros de carte de crédit ou de compte bancaire, sans que vous le sachiez.

Les arnaques vous incitent à fournir volontairement des informations personnelles par le biais de tactiques telles que les courriels d'hameçonnage, les faux comptes de médias sociaux et les offres trop belles pour être vraies.

Les fraudes et arnaques en ligne constituent un problème significatif, car elles peuvent gêner, ou même détruire, votre vie financière, personnelle et professionnelle.

1.

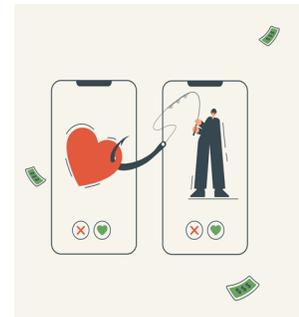
Remplissez les tirets pour que les phrases aient un sens.  
(Compétences numériques, niveau intermédiaire)

Lors d'une \_\_\_\_\_, un pirate informatique \_\_\_\_\_ vos informations, généralement \_\_\_\_\_.

Lors d'une \_\_\_\_\_, on vous incite à \_\_\_\_\_ des informations \_\_\_\_\_.

## TYPES D'ARNAQUES LES PLUS COURANTES

Selon le Bureau de l'Ombudsman canadien des services bancaires et d'investissement (OSBI), les arnaques en ligne les plus courantes au Canada sont liées aux relations amoureuses, à l'emploi et au magasinage en ligne.





Les arnaques liées aux relations amoureuses ont souvent lieu sur des sites de rencontre en ligne ou d'autres médias sociaux. Le fraudeur crée un faux profil en ligne, en utilisant souvent une identité volée. Il prétend aussi souvent avoir un emploi prestigieux qui l'oblige à voyager beaucoup. Il peut ainsi dire plus tard que c'est la raison pour laquelle il ne peut pas vous rencontrer en personne.

En somme, l'arnaqueur identifie une personne qui semble prête à établir une relation et la charme en ligne jusqu'à ce qu'elle ait l'impression de faire partie d'une véritable relation. Une fois que l'arnaqueur a gagné la confiance de sa victime, il lui dit avoir besoin d'emprunter une petite somme d'argent pour faire face à une situation urgente. Les montants deviennent de plus en plus importants jusqu'à ce que, dans de nombreux cas, l'arnaqueur emprunte une très grosse somme. Éventuellement, la victime peut tout perdre lorsque l'arnaqueur disparaît.



Arnaque à l'emploi

Les arnaques liées à l'emploi apparaissent souvent sur des sites d'offres d'emploi, des sites de réseaux sociaux tels que Facebook et Twitter (X). Ou encore, les cibles de ces arnaques peuvent recevoir des courriels non sollicités de la part de prétendus employeurs. L'arnaqueur se fait souvent passer pour une entreprise légitime et propose un emploi « trop beau pour être vrai » à la victime ; il lui propose un poste bien rémunéré et qui peut généralement être exercé à domicile. Cette offre donne à la victime l'impression d'être importante.

Dans cette arnaque, la victime envoie volontairement les informations personnelles demandées, telles que son numéro d'assurance sociale, sa carte d'identité avec photo ou son numéro de compte bancaire, afin d'y faire le dépôt automatique de son salaire. Le « nouvel employé » peut être invité à recevoir de l'argent et à en renvoyer à d'autres personnes de la « société ». On peut aussi lui demander de rembourser de l'argent parce que son salaire a été mal calculé. La victime peut aussi se faire voler toute son identité.

Le magasinage en ligne est le troisième grand type d'arnaque. Les arnaques liées à l'achat d'articles en ligne sont l'une des fraudes les plus courantes qui touchent les adolescents et les jeunes adultes.

Lorsque vous achetez, les vendeurs frauduleux peuvent proposer des produits, mais ne jamais vous les envoyer après que vous les avez payés.

Lorsque vous vendez, les acheteurs frauduleux peuvent vous envoyer un faux chèque, un faux mandat ou un faux virement bancaire. Parfois, ils peuvent payer trop cher en utilisant l'un de ces faux types de paiement et vous demander ensuite de leur envoyer la différence ou de les rembourser complètement.



Le magasinage en ligne en toute sécurité n'est pas très différent de l'achat dans un magasin physique que vous connaissez bien. Privilégiez les entreprises en ligne que vous connaissez et en qui vous avez confiance, en particulier pour les achats importants tels que les appareils électroniques, les gadgets et les cartes-cadeaux.



Si vous devez magasiner sur un nouveau site Web, il y a toutefois quelques éléments à vérifier pour vous assurer que vous ne serez pas victime d'une arnaque :

Ne sauvegardez pas les informations liées à votre carte de crédit dans votre navigateur Web.

- Même si cela permet de gagner quelques secondes, le fait d'enregistrer les informations en lien avec votre carte de crédit dans votre navigateur signifie que toute personne ayant accès à votre appareil ou à vos comptes peut effectuer des achats avec votre carte. Cette situation est encore plus préoccupante si des cybercriminels compromettent ou piratent votre appareil.

Vérifiez régulièrement vos comptes bancaires et vos relevés de carte de crédit.

- Si vous effectuez des achats en ligne, il est important de vérifier fréquemment vos relevés pour vous assurer que vous n'êtes pas victime d'une arnaque. Si vous payez par carte de débit, n'oubliez pas de vérifier le compte auquel elle est rattachée. Si vous remarquez des frais suspects ou inattendus sur vos relevés, contactez immédiatement la banque ou la compagnie de votre carte de crédit.

Édité et traduit. Source : <https://www.obsi.ca/en/news/online-scams-are-cheating-a-growing-number-of-consumers-out-of-their-savings.aspx>

1.

À l'aide des informations que vous venez de lire, placez un X dans les colonnes correspondant à chaque technique et au type d'arnaque pour lequel elle est le plus souvent utilisée.

Attention, des arnaques différentes peuvent utiliser les mêmes techniques.

*(Compétences numériques, niveau intermédiaire)*

TECHNIQUE	RELATIONS AMOUREUSES	EMPLOI	MAGASINAGE
Gagner votre confiance			
Offrir quelque chose de trop beau pour être vrai			
Envoyer un faux transfert d'argent			
Demander des informations d'identification personnelle			
Indiquer que c'est urgent			
Ne pas envoyer ce qui a été promis			
Vous donner l'impression d'être important			
Demander un type de paiement inhabituel			
Effectuer le premier contact via les médias sociaux			



2.

À l'aide des informations fournies dans la boîte de texte, quelles images ou quels mots affichés sur un site Web vous indiquent que vous pouvez y magasiner avec votre carte de crédit en toute sécurité ? Cochez toutes les cases correspondantes.

*(Compétences numériques, niveau intermédiaire)*

Magasiner sur un site Web sécurisé

1. Un crochet vert
2. Le mot sécurisé
3. Le mot buysafe
4. Un symbole de serrure
5. Un crochet rouge
6. Le mot http
7. Le mot ccsafe
8. Le mot https
9. Le mot safe
10. Le mot SSL



N'achetez jamais rien en ligne avec votre carte de crédit sur un site qui n'est pas équipé du système de cryptage SSL (*secure sockets layer*—couches d'échange sécurisées). Vous saurez que le site utilise le protocole SSL parce que l'URL du site commencera par HTTPS — au lieu de HTTP. Une icône représentant un cadenas verrouillé apparaît également, généralement à gauche de l'URL dans la barre d'adresse ou dans la barre au-dessous ; cela dépend de votre navigateur. Le protocole HTTPS est maintenant la norme sur les sites qui ne sont pas destinés au magasinage, au point que Google Chrome signale toute page sans S comme « non sécurisée ».

3.

Consultez au moins deux sites Web sur lesquels vous avez effectué des achats et répondez aux questions suivantes pour chacun d'entre eux.

*(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier.*

Site Web 1

Nom de l'entreprise : \_\_\_\_\_

URL du site Web : \_\_\_\_\_

La page de paiement commence-t-elle par https ? Oui \_\_\_ Non \_\_\_

La page de paiement a-t-elle une icône de cadenas ? Oui \_\_\_ Non \_\_\_



Avez-vous enregistré les données de votre carte de crédit sur le site ? Oui \_\_\_\_ Non \_\_\_\_

(Si oui, pensez à les supprimer maintenant).

Site Web 2

Nom de l'entreprise : \_\_\_\_\_

URL du site Web : \_\_\_\_\_

La page de paiement commence-t-elle par https ? Oui \_\_\_\_ Non \_\_\_\_

La page de paiement a-t-elle une icône de cadenas ? Oui \_\_\_\_ Non \_\_\_\_

Avez-vous enregistré les données de votre carte de crédit sur le site ? Oui \_\_\_\_ Non \_\_\_\_

(Si oui, pensez à les supprimer maintenant).

## RECONNAITRE LES ARNAQUES EN LIGNE

En plus de vérifier les sites Web lorsque vous effectuez des paiements, soyez attentif à ces signes indiquant qu'il pourrait s'agir d'une arnaque :

- Le contact est inattendu.
- L'offre semble trop belle pour être vraie — c'est une réduction ou une offre bien plus intéressante que ce à quoi vous vous attendiez.
- On vous demande de fournir des informations personnelles.
- On vous demande d'effectuer un paiement, quel qu'il soit.
- On vous demande d'effectuer un paiement sous une forme inhabituelle et spécifique (par exemple, un virement bancaire ou un ordre de virement).
- On vous demande de faire quelque chose rapidement, sinon vous risquez de rater l'affaire.

1.

Faites la lecture de chaque scénario et identifiez dans chacun d'eux au moins 3 indices qui auraient dû aider la victime à reconnaître qu'on tentait de l'arnaquer. Inscrivez vos réponses dans les espaces fournis.

*(Compétences numériques, niveau intermédiaire)*

### Scénario 1

À la dernière minute, Karrie a voulu acheter deux billets pour un festival de musique d'été. Toutefois, le site Web officiel indiquait qu'il n'y avait plus de places disponibles. Elle a trouvé quelqu'un en ligne qui avait deux billets disponibles pour 150 \$ chacun. Elle a pensé que c'était une très bonne affaire et a accepté d'envoyer 300 dollars en utilisant PayPal. Le



vendeur a déclaré qu'il préférerait les cartes-cadeaux parce qu'il avait déjà été victime d'une arnaque et qu'il savait maintenant que les cartes-cadeaux étaient « plus sûres » que PayPal. Il a également dit qu'il était vraiment désolé de ne pas pouvoir aller au festival, mais qu'il avait un besoin urgent de vendre les billets. Il a ajouté qu'il ne pouvait pas les garder en attendant qu'elle prenne une décision. Karrie a trouvé cela étrange, mais le type avait l'air sympa. Elle a donc accepté et a acheté trois cartes-cadeaux de 100 \$ en ligne et lui a envoyé les informations. Une fois les cartes échangées, il l'a immédiatement bloquée sur Facebook. Finalement, elle n'avait pas de billets, pas de remboursement, et aucun moyen de retrouver l'homme en question.

Identifiez au moins 3 indices

---

---

---

### Scénario 2

Devrin venait de commencer son premier véritable emploi après l'école et voulait offrir un cadeau à ses parents pour les remercier de leur aide au fil des ans. Sachant que le barbecue familial commençait à se faire vieux, Devrin a cherché une bonne affaire en ligne. Il a trouvé un site Web qui proposait des barbecues de marque à des prix ridiculement réduits. Le site indiquait qu'il s'agissait d'une nouvelle entreprise, que les bas prix faisaient partie de leurs promotions de lancement et qu'il s'agissait d'une « offre à durée limitée ». La seule condition était de faire une demande de crédit et de payer avec la carte de crédit de l'entreprise. Le taux de la carte était très compétitif, à seulement 2,9 %. Devrin a effectué une recherche en ligne sur l'entreprise et n'a pas trouvé de mauvaises critiques. Il a donc demandé la carte sur le site Web de l'entreprise et l'a utilisée pour payer le barbecue. Une semaine plus tard, il a reçu un courriel l'informant qu'en raison de problèmes liés à la chaîne d'approvisionnement, la livraison du barbecue avait été retardée. On lui a aussi indiqué que, puisque l'entreprise n'était pas responsable de ce retard, il ne pouvait pas obtenir un remboursement. Devrin est immédiatement retourné voir le site Web de l'entreprise, mais celui-ci avait disparu. Le barbecue n'a jamais été livré et il n'a jamais été remboursé.

Identifiez au moins 3 indices

---

---

---



### Scénario 3

Alix a rencontré son partenaire Seamus sur Facebook. Ils ont échangé des textos et clavardé en ligne pendant plusieurs mois, et leur relation est devenue plus sérieuse au fil du temps. Seamus a déclaré qu'il vivait en Irlande, mais qu'il était prêt à déménager au Canada pour voir où leur relation pourrait aller. Il a envoyé à Alix les informations concernant son vol et lui a dit qu'il avait déjà expédié ses affaires. Le jour du vol, Alix a reçu un appel d'un agent des douanes lui annonçant que la cargaison était arrivée, mais qu'il fallait payer les douanes. On lui a dit qu'on avait essayé de joindre Seamus, mais qu'on n'avait pas pu le faire, car il était en transit. Le numéro d'Alix se trouvait sur la cargaison en tant que personne à contacter au Canada, ils ont donc décidé de la joindre. Les douanes ont expliqué que si les douanes n'étaient pas payées immédiatement, la cargaison serait renvoyée en Irlande aux frais de Seamus. Alix a voulu aider et a donc payé le solde dû par virement bancaire, conformément aux instructions, pour un montant de 3 355,99 dollars. Elle avait déjà prêté de petites sommes d'argent à Seamus, qui les avait toujours remboursées. Elle ne s'inquiétait donc pas.

Quand Alix est arrivée à l'aéroport ce soir-là pour rencontrer Seamus, il ne s'est pas présenté. Lorsqu'elle a essayé de lui envoyer un message, il n'a pas répondu. Son profil Facebook est aussi disparu. Quelques jours plus tard, Alix s'est rendu compte qu'elle avait été victime d'une arnaque. Elle a demandé à sa banque de récupérer le paiement, mais l'argent avait déjà été transféré et elle n'a pas obtenu gain de cause.

Identifiez au moins 3 indices

---

---

---



## POURQUOI LES ARNAQUES FONCTIONNENT-ELLES ?

Les arnaques fonctionnent pour deux raisons principales.

1. Les gens sont pressés.
2. Les arnaqueurs sont intelligents et savent comment manipuler les gens.

La quantité d'informations numériques qui nous parvient chaque jour est énorme. La technologie numérique facilite non seulement l'accomplissement de nombreuses tâches quotidiennes, mais elle en accélère également l'exécution. Nous avons donc l'impression que nous devons être plus rapides, que nous devons toujours répondre immédiatement. Selon Malawarebytes, 70 % des messages analysés qui étaient liés à une arnaque contenaient un message du type « Dépêchez-vous s'il vous plait ». Les recherches confirment que cette augmentation du volume et de la vitesse a un effet très négatif sur notre durée d'attention, qui est tombée à moins de 8 secondes ! La réduction de la durée d'attention signifie que les gens prennent rarement connaissance de tous les détails d'un message.



Compte tenu du volume, de la vitesse et de la courte durée d'attention, sans oublier que tout le monde utilise son téléphone portable pour effectuer des opérations bancaires, magasiner, prendre des rendez-vous, etc., il est normal de recevoir un texte ou un courriel d'un fraudeur et de croire qu'il est légitime.

Les arnaqueurs sont intelligents. La plupart des arnaqueurs ne correspondent pas à l'image stéréotypée d'un « geek » installé dans le sous-sol de ses parents. Ils peuvent faire partie de réseaux sophistiqués de personnes travaillant ensemble. Qu'ils soient seuls ou avec d'autres, ils comprennent non seulement que les gens ont une durée d'attention courte et comment utiliser les faiblesses de la technologie numérique à leur avantage, mais ils ont également une bonne connaissance de la façon dont les gens pensent, ce qu'ils utilisent à notre détriment. C'est ce qu'on appelle la manipulation psychologique, et elle peut fonctionner sur n'importe qui.

Les arnaqueurs sont très habiles à manipuler les gens pour obtenir ce qu'ils veulent. Par exemple, ils peuvent vous faire dévoiler des informations personnelles ou vous convaincre de leur donner de l'argent. Pour ce faire, ils utilisent des tactiques qui exploitent les penchants et les sentiments normaux de l'être humain. Les arnaqueurs savent que la plupart des gens veulent se sentir valorisés et éviter de vivre des choses désagréables ; ils peuvent donc vous suggérer :

- De faire confiance à quelqu'un parce qu'il semble sympathique.
- De faire confiance à quelqu'un parce qu'il dit que vous êtes spécial et qu'il vous aime bien.
- De faire les mêmes choses que les autres pour ne pas avoir peur de manquer quelque chose.
- D'obéir à une figure d'autorité.
- D'éviter la punition ou l'embarras.
- De vouloir quelque chose parce que c'est rare et que tout le monde ne peut pas l'avoir.
- D'agir rapidement parce que c'est urgent ou que le temps est limité.



1.

Cochez toutes les affirmations pertinentes.  
(Compétences numériques, niveau intermédiaire)

LES FRAUDES SONT POSSIBLES, CAR :	✓
Les gens sont stupides	
Les gens veulent faire de bonnes affaires	
Les gens utilisent des téléphones portables	
Les arnaqueurs sont intelligents	
Les gens aiment se sentir spéciaux	
Les gens ne reçoivent pas assez de courriels	
Les arnaqueur savent comment manipuler les gens	

2.

Indiquez si les affirmations ci-dessous sont vraies ou fausses.  
(Compétences numériques, niveau intermédiaire)

AFFIRMATIONS	VRAI	FAUX
La durée d'attention typique est de 8 minutes.		
La peur de manquer sa chance est une cause réelle d'arnaque.		
Toute personne âgée utilisant Internet peut être victime d'une arnaque.		
La manipulation psychologique ne fonctionne pas.		
Certaines personnes se font piéger parce qu'elles sont seules.		
Seuls 7 % des courriels frauduleux sont urgents.		
Certaines personnes se font arnaquer parce qu'elles se croient plus intelligentes que les autres.		



## QUE SE PASSE-T-IL SI VOUS PAYEZ ACCIDENTELLEMENT UN ARNAQUEUR ?

Si vous payez accidentellement un arnaqueur, il y a des choses que vous pouvez et devez faire immédiatement. Bien que vous ne puissiez pas toujours récupérer votre argent, en signalant l'arnaque, vous pouvez vous assurer que quelqu'un d'autre ne tombera pas dans le même piège.

### 1. Parlez-en à quelqu'un !

- a. La fraude est un crime ! Rassemblez toutes les informations relatives à la fraude. Il peut s'agir de documents, de reçus, de copies de courriels et/ou de textes. Partagez-les avec la police, surtout si vous avez perdu de l'argent.
- b. Signalez la fraude au centre anti-fraude ou au bureau de la concurrence.
- c. Informez le site Web ou la place de marché en ligne où la fraude a eu lieu.
- d. Informez votre banque ou votre institution financière et la compagnie qui émet votre carte de crédit.



### 2. Comment avez-vous perdu l'argent ? Le type de méthode de paiement que vous avez utilisé a une incidence sur ce que vous devez faire ensuite.

- a. Avez-vous payé avec votre carte de crédit ou de débit ? Signalez toujours à votre banque tout montant frauduleux débité de votre carte et demandez-lui de l'annuler.
- b. Avez-vous payé avec une carte-cadeau ? Contactez immédiatement l'entreprise qui émet la carte-cadeau et informez-la de cette fraude. Conservez des copies des cartes-cadeaux et de leurs reçus à des fins de référence.
- c. Avez-vous effectué un virement bancaire ? Signalez le virement à votre banque dès que possible. Demandez-lui de vous indiquer la procédure à suivre pour annuler un virement bancaire.
- d. Avez-vous utilisé une application de transfert de fonds ? Contactez l'entreprise propriétaire de l'application et signalez l'arnaque. Renseignez-vous pour savoir s'ils ont une politique qui vous permet d'annuler le paiement et de récupérer votre argent.
- e. Avez-vous payé avec de la cryptomonnaie ? Si vous avez utilisé une bourse d'échange centralisée, signalez-lui la fraude et demandez-lui s'il est possible d'annuler votre paiement.



1.

Faites correspondre le type de paiement utilisé avec l'endroit où vous devez le signaler si vous êtes victime d'une fraude. Certaines réponses peuvent être utilisées plusieurs fois.  
(Compétences numériques, niveau intermédiaire)

Type de paiement	Signalez la fraude à ...
Application de transfert de fonds	
Carte de crédit	
Virement bancaire	
Carte-cadeau	
Cryptomonnaie	

La bourse d'échange

Votre banque

L'entreprise qui émet la carte-cadeau

L'entreprise propriétaire de l'application

LA FRAUDE AU TRAVAIL



Reconnaitre les arnaques et les fraudes en ligne au travail est tout aussi important que dans votre vie personnelle. Si vous communiquez en ligne dans le cadre de votre travail, vous devez respecter toutes les politiques de l'employeur en matière de communication numérique. C'est le cas lorsque vous envoyez des courriels ou des textos à vos collègues et à vos clients, mais c'est particulièrement vrai si une partie de votre travail consiste à effectuer des achats en ligne pour votre employeur ou à partager des informations financières en ligne. Examinons le cas

suivant.

Une entreprise de transport de taille moyenne a reçu un courriel de l'un de ses fournisseurs. Le fournisseur indiquait que la banque a mis à jour les informations relatives au compte lui permettant de recevoir des paiements et qu'elle avait inclus le numéro de compte. On lui demandait si les paiements pouvaient être versés à ce nouveau compte et on s'excusait pour



le désagrément. Le courriel contient une facture de ce qui a été fourni ce mois-là, ainsi que les courriels échangés entre l'entreprise et le fournisseur.

Tout semble être une copie parfaite des factures qu'elle avait reçues auparavant, de sorte que l'entreprise de transport a envoyé le paiement de plus de 80 000 dollars au nouveau compte sans trop lui accorder d'attention. Malheureusement, le véritable fournisseur n'a jamais reçu le paiement.

Il s'est avéré que les fraudeurs avaient piraté le service informatique du fournisseur pour accéder à d'anciens courriels et à des informations de compte pour ensuite créer une fausse facture. Comme les fraudeurs utilisaient la véritable adresse électronique du fournisseur, mais qu'ils avaient réussi à intercepter et à dissimuler les courriels de l'entreprise, le fournisseur ne les a jamais reçus non plus. L'entreprise n'a rien découvert jusqu'à ce que le fournisseur la contacte par téléphone pour lui demander pourquoi la facture n'avait pas été payée.

*Il s'agit ici d'une arnaque très sophistiquée, et le seul véritable indice était qu'il s'agissait d'un changement d'informations bancaires. Le meilleur moyen d'éviter cette situation aurait été que l'employeur adopte une politique stipulant que, lorsque des informations bancaires sont impliquées, il faut contacter directement le fournisseur en utilisant un second mode de communication fiable, comme un numéro de téléphone connu, afin de vérifier la demande.*

Édité et traduit. Source : <https://www.scamwatch.gov.au/protect-yourself/real-life-stories/scam-victims-tell-us-their-stories/business-email-compromise-our-business-lost-190-000-when-our-suppliers-email-was-hacked>

---

## POUR EN APPRENDRE D'AVANTAGE

Le gouvernement du Canada reconnaît que la fraude en ligne représente un problème important pour les personnes et les entreprises.

Consultez les sites suivants pour obtenir les informations les plus récentes sur les arnaques qui existent et sur la manière de se protéger.

- Bureau de la concurrence du Canada : Le petit livre noir de la fraude, 2<sup>e</sup> édition. Édition — disponible dans plusieurs langues.  
<https://ised-isde.canada.ca/site/bureau-concurrence-canada/sites/default/files/attachments/2022/CB-LBBS2-FR.pdf>
- Pensez cybersécurité. <https://www.pensezcybersecurite.gc.ca/fr>
- Agence du revenu du Canada : arnaques et fraudes.  
<https://www.canada.ca/en/revenue-agency/campaigns/fraud-scams.html>







## 5. UTILISER L'IA

### Le monde de l'IA

L'intelligence artificielle (IA) est l'une des plus grandes révolutions de la technologie numérique. L'utilisation de la technologie de l'IA progresse à un rythme phénoménal. Des choses que l'on considérait comme de la science-fiction, il y a à peine dix ans, comme les voitures autopilotées, font maintenant partie de notre réalité. Il y a de fortes chances que vous utilisiez déjà l'IA quotidiennement ; il se peut même qu'elle prenne de plus en plus de place dans votre vie personnelle et professionnelle. Comme la plupart des technologies numériques, l'IA n'est ni bonne ni mauvaise ; tout dépend de la manière dont on l'utilise.

### L'IA en quelques mots

- L'IA, abréviation d'intelligence artificielle, est la science qui consiste à fabriquer des machines capables de penser comme des humains. L'IA rend les machines « intelligentes ».
- Dans les années 1950, l'informaticien Alan Turing a réalisé le premier grand test visant à déterminer si les machines pouvaient être intelligentes. Le terme « IA » a été utilisé pour la première fois lors d'une conférence en 1955.
- L'IA utilise des « algorithmes », qui sont des ensembles de règles programmées par des humains dans des ordinateurs. L'IA peut adapter ces algorithmes, de sorte qu'ils deviennent plus intelligents et plus rapides au fur et à mesure qu'ils sont utilisés et qu'ils analysent davantage de données. Les ordinateurs « apprennent » de cette manière.
- Au Canada, l'utilisation de l'IA est une responsabilité fédérale et, en octobre 2023, le gouvernement a publié un code de conduite volontaire pour l'utilisation des systèmes d'IA générative, qui comprend un engagement à la transparence et à l'absence de préjugés. L'IA générative comprend des produits comme ChatGPT et d'autres systèmes qui peuvent créer des choses (les générer) comme du texte, des images, de la musique ou des vidéos. Ce code de conduite s'applique à tous les types d'entreprises.



## UNE PENSÉE INTELLIGENTE !

La technologie SMART est alimentée par l'IA. SMART est l'acronyme de « *Self-Monitoring, Analysis and Reporting Technology* » (technologie d'autocontrôle, d'analyse et permettant d'émettre des rapports), mais cette technologie est aussi généralement qualifiée d'« intelligente », car elle rend des objets tels que les téléphones et d'autres technologies plus intelligents.



Alors, dans quel domaine de la vie les gens pensent-ils que l'utilisation de l'IA engendrera les changements les plus importants ?



Les informations ci-dessous sont basées sur un graphique de 2021 publié par Statista. (<https://www.statista.com/chart/29229/areas-of-life-most-expected-to-change-by-the-use-of-ai/>)

Le graphique décrit les domaines de la vie qui, selon les personnes interrogées, changeront le plus à cause de l'utilisation accrue de l'IA entre 2021 et 2026. L'échantillon de population participant à l'étude était composé de 19 504 personnes âgées de 16 à 74 ans originaires de 28 pays. Utilisez les informations pour répondre aux questions.

*(Compétences numériques, niveau intermédiaire)*

Pourcentage des personnes interrogées qui s'attendent à ce que les domaines suivants subissent les changements les plus importants en raison de l'utilisation de l'IA au cours des 3 à 5 prochaines années.

35 % — Éducation	32 % — Emploi
30 % — Transport	26 % — Cout de la vie
23 % — Salaires	15 % — Nourriture et nutrition
33 % — Sécurité	31 % — Magasinage
27 % — Divertissement	23 % — Foyer
22 % — Environnement	15 % — Relations personnelles

Quel est le domaine pour lequel la plupart des gens pensent qu'il y aura le plus grand changement ?

---

Quel est le domaine dans lequel vous pensez que les changements seront les plus importants ? Justifiez votre réponse.

---



---

---

Quel est le domaine pour lequel la plupart des gens pensent qu'il y aura le moins de changements ?

Quel est le domaine pour lequel vous pensez qu'il y aura le moins de changements ? Justifiez votre réponse.

---

---

## QUE SAVEZ-VOUS DÉJÀ AU SUJET DE L'INTELLIGENCE ARTIFICIELLE ?

Vous n'avez peut-être pas de voiture autopilotée, mais si vous avez déjà demandé à Alexa à quelle heure commence un film ou utilisé un filtre Snapchat pour transformer votre photo de profil en dessin animé, vous utilisez déjà l'IA.

Découvrez comment Morgan utilise l'IA tous les matins.

Chaque matin, lorsque Morgan se réveille, il attrape son téléphone intelligent, le place devant son visage pour se connecter et voir ce qui s'est passé pendant qu'il dormait. Il clique sur les médias sociaux, fait défiler les premiers messages et vérifie s'il y a reçu de nouvelles demandes d'amis. Il consulte sa montre intelligente pour savoir comment il a dormi et son calendrier pour savoir s'il a des réunions. Il recherche l'itinéraire le plus rapide pour se rendre dans un établissement où il n'est jamais allé, constate qu'il y a des travaux et envoie un message à son collègue pour l'informer du détour recommandé et du temps de plus dont il aura besoin. Cela fait beaucoup d'intelligence artificielle, et tout cela avant même de sortir du lit.

- 1.** Dressez la liste de tous les types d'IA que Morgan a utilisés, selon vous, avant de se lever du lit. Vérifiez vos réponses à la page suivante.  
*(Compétences numériques, niveau intermédiaire)*





Voici la liste de l'IA que Morgan a utilisée ce matin-là. Combien en avez-vous obtenu ?

- **Téléphone intelligent** : Le téléphone intelligent de Morgan est doté d'une IA. C'est ce qui le rend « intelligent ».
- **Reconnaissance du visage** : FaceID utilise la biométrie de l'IA et des algorithmes d'apprentissage automatique pour comparer le balayage de votre visage avec ce qu'il a enregistré à son sujet afin de déterminer si c'est bien vous qui tentez de déverrouiller le téléphone.
- **Recommandations personnalisées** : L'IA détermine quels messages vous voyez à quel moment, de sorte que vos médias sociaux sont personnalisés en fonction de vos centres d'intérêt passés, ce qui vous incite à y passer plus de temps.
- **Outils intelligents (SMART)** : Les montres intelligentes utilisent l'intelligence artificielle pour suivre les données biométriques et donner des conseils en cas de changement dans l'état de santé.
- **GPS** : Les applications de cartographie utilisent l'IA pour suivre les itinéraires et les événements en temps réel.
- **Outils de rédaction** : Les courriels et les communications textuelles sont améliorés par des outils d'IA tels qu'Antidote et le texte prédictif.
- **Logiciel antivirus** : Les logiciels antivirus utilisent l'IA pour bloquer les pourriels et s'assurer que vos messages arrivent en toute sécurité.

Voici quelques autres exemples d'utilisation de l'IA au quotidien comprenant plus de détails et accompagnés d'un avantage et d'un inconvénient pour chacun d'entre eux.

#### ASSISTANTS VIRTUELS

- Les assistants intelligents comme Alexa d'Amazon, Siri d'Apple et Google Assistant utilisent des technologies d'IA pour interpréter les commandes vocales, répondre aux questions et exécuter des tâches. Ces assistants utilisent des algorithmes de traitement du langage naturel et d'apprentissage automatique pour comprendre l'intention de l'utilisateur, récupérer des informations pertinentes et exécuter les actions demandées.





- **Avantage :** Ils fournissent des réponses à des questions de base rapidement. Ces réponses sont généralement très exactes.
- **Désavantage :** Les assistants virtuels sont toujours « à l'écoute ». L'utilisation qu'ils font de ces données présente des risques pour la vie privée. (Vous pouvez en apprendre davantage sur la protection de la vie privée dans la séance de formation : Mots de passe et cybersécurité).



## SE RENDRE AU TRAVAIL

- Les voitures autopilotées s'appuient fortement sur l'IA pour percevoir, prendre des décisions et contrôler. Grâce à une combinaison de capteurs, de caméras et d'algorithmes d'apprentissage automatique, ces véhicules peuvent détecter des objets, interpréter les panneaux de signalisation et naviguer dans des conditions routières complexes de manière autonome, améliorant ainsi la sécurité et l'efficacité sur les routes. Google maps et d'autres applications de voyage utilisent l'IA pour surveiller la circulation afin de vous communiquer des informations en temps réel sur celle-ci et au sujet des conditions météorologiques, lui permettant ainsi de vous suggérer des moyens d'éviter les embouteillages.
- **Avantage :** Le GPS dans les applications pour téléphones et voitures permet de considérablement gagner du temps ; de plus, ses fonctions vocales signifient que les conducteurs ne doivent pas se contenter des informations affichées à l'écran.
- **Désavantage :** Aujourd'hui, les véhicules autopilotés sont très coûteux et risquent d'être impliqués dans des accidents. Toutefois, ils sont de moins en moins dispendieux et de plus en plus sécuritaires.

## RECOMMANDATIONS POUR LA DIFFUSION EN CONTINU ET LE MAGASINAGE

Le magasinage en ligne est une autre façon dont de nombreuses personnes sont régulièrement exposées à l'intelligence artificielle. Les algorithmes d'IA des fournisseurs surveillent ce que vous achetez et ce qu'achètent d'autres personnes qui, selon l'IA, vous ressemblent, afin de vous faire des recommandations lorsque vous visitez leurs sites. Les services de diffusion en continu fonctionnent de la même manière. Les moteurs de recommandation des entreprises sont alimentés par l'IA et utilisent votre historique de visionnement pour vous offrir des suggestions sur ce que vous pourriez vouloir regarder (y compris les genres, les acteurs, les périodes, etc.) Cet outil permet d'être aussi précis, et même noter le moment où vous avez regardé quelque chose et ce que vous avez l'habitude de regarder pendant cette période. En fait, 80 % de ce que nous regardons est déterminé par les recommandations de Netflix.



- **Avantage :** Vous pouvez facilement voir des produits et des suggestions de films qui pourraient vous intéresser.
- **Désavantage :** On peut vous convaincre d'acheter des articles ou de louer des films que vous n'aviez pas l'intention d'acheter.



1.

Réfléchissez à deux types d'IA que vous utilisez et écrivez-les en indiquant ce que vous pensez être un avantage et un inconvénient pour chacun d'entre eux. Ne répétez pas les avantages et les inconvénients mentionnés dans l'article précédent.

(*Compétences numériques, niveau intermédiaire*) Les réponses peuvent varier.

AI n° 1 :

---

---

---

AI n° 2 :

---

---

---

ET MAINTENANT, VOICI LE DERNIER-NÉ DE LA FAMILLE : ChatGPT !

En 2023, même les personnes qui ne connaissaient rien à l'intelligence artificielle ont soudainement entendu parler de ChatGPT. Depuis qu'il a été présenté aux consommateurs en 2022 sous forme d'un logiciel gratuit à télécharger, ChatGPT connaît un véritable succès. Qu'est-ce que c'est ?

Le nom ChatGPT est l'acronyme de *Chat Generative Pre-trained Transformer* (transformateur génératif préentraîné). C'est un *dialogueur* (chatbox — un programme informatique conçu pour simuler une conversation avec des utilisateurs humains, notamment sur Internet) très intelligent. Il est conçu pour fournir des réponses naturelles et fluides aux humains. Le *dialogueur* a été créé sur la base d'une technologie d'apprentissage automatique, ce qui signifie qu'il peut s'adapter à différentes situations et interactions pour dispenser une expérience plus personnalisée et plus efficace.



ChatGPT ne se limite pas à fournir des réponses comme le font les assistants virtuels. Il personnalise ces réponses en y ajoutant des couches d'émotions et d'expériences humaines. Par exemple, les utilisateurs peuvent demander à ChatGPT de rédiger des « vœux de mariage sincères et bien sentis » ou des avis nécrologiques « sérieux, mais avec un peu d'humour à l'ancienne ». ChatGPT peut aussi rédiger des travaux scolaires tels que des articles qui « décrivent l'histoire des outils manuels de menuiserie au



Canada en utilisant le modèle de l'essai en 5 paragraphes qui semblent avoir été rédigés par un élève de 9<sup>e</sup> année ».

Les enseignants du secondaire, les professeurs du postsecondaire, les parents et les apprenantes se posent tous des questions au sujet de l'utilisation de ChatGPT :

- Plagiat : ChatGPT encourage-t-il les apprenants à tricher ?
- Éthique : ChatGPT encourage-t-il les apprenants à penser qu'il est acceptable d'utiliser les idées des autres ?
- Désinformation : Comment ChatGPT sait-il si l'information qu'il partage est vraie ?
- Préjugés : ChatGPT transmet-il les préjugés des personnes qui l'utilisent ?

**2.**

Il est important de connaître le sens de ces différents mots dans le contexte de l'IA. Dans le tableau suivant, associez à chaque mot la définition qui vous semble la plus appropriée, en traçant une ligne entre les deux.

*(Compétences numériques, niveau intermédiaire)*

MOTS	DÉFINITIONS
Plagiat	Faits faux ou inexacts.
Éthique	Prédictions ou résultats qui favorisent ou discriminent des groupes spécifiques de personnes.
Désinformation	Lorsqu'une personne présente un certain type de travail comme étant sa propre création alors qu'en réalité il ne s'agit pas de son travail.
Biais	Lorsqu'une personne fait quelque chose de malhonnête dans le cadre d'un travail académique ou professionnel qui donne une fausse représentation de ce qu'elle comprend ou de ce qu'elle peut faire, lui procurant ainsi un avantage injuste.
Tricherie	Ensemble de principes moraux suivis par des personnes généralement considérées comme bonnes.



Les écoles et les établissements d'enseignement postsecondaire auront probablement leur propre définition du plagiat et de la tricherie. Il est possible que l'on encourage une utilisation plus éthique de la technologie plutôt que d'en restreindre l'usage. Le maintien d'une bonne éthique est une partie importante de la vie d'un étudiant et d'un professionnel.

3.

Consultez le graphique de la page suivante, créé pour les enseignants, qui montre comment les élèves utilisent l'IA comme ChatGPT. Parmi les actions de droite, lesquelles vous semblent être de la tricherie ?

*(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier.*

---



---



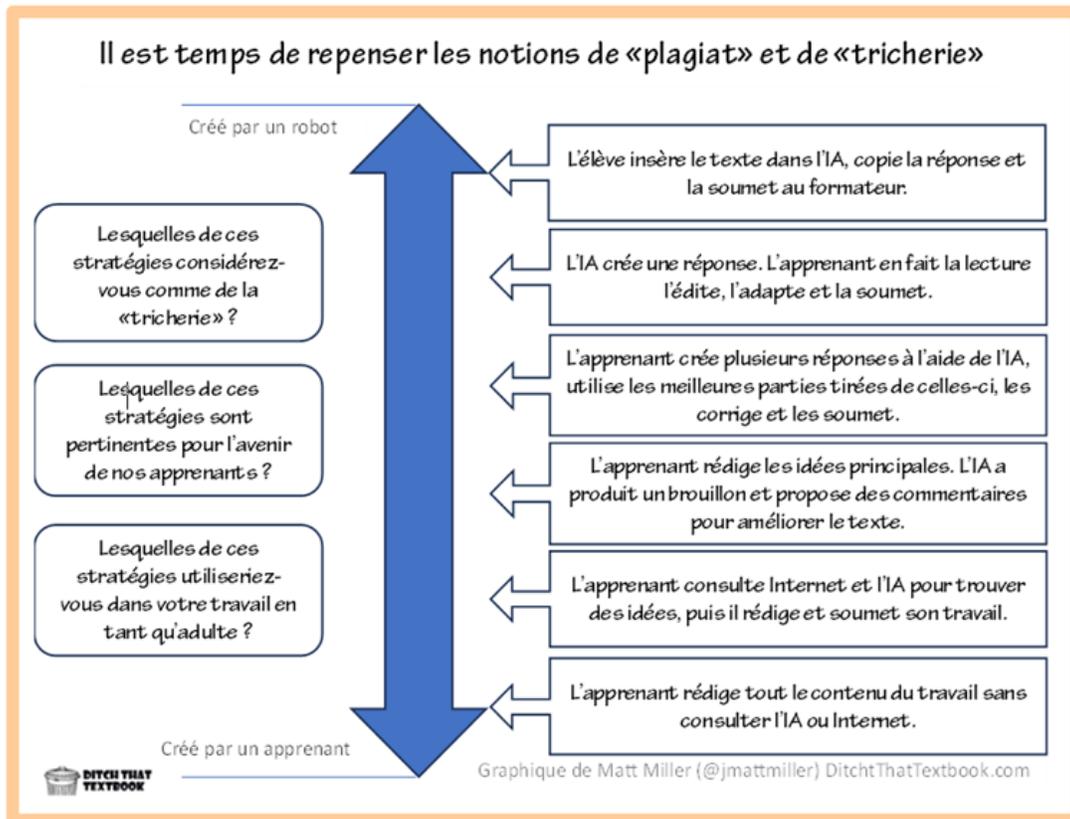
---



---



---



<https://ditchthattextbook.com/ai/>



4.

Rédigez trois règles simples qui, selon vous, seraient utiles pour aider les apprenants à comprendre quand ils peuvent utiliser le ChatGPT et pour s'assurer que son utilisation se fait dans le respect de l'éthique.

*(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier.*

---

---

---

---

---

---

---

---

5.

Examinez cette utilisation réelle en lien avec l'IA, rapportée dans le Toronto Life Magazine, et répondez aux questions qui suivent.

*(Compétences numériques, niveau intermédiaire)*

En février 2023, un étudiant en sciences de la Terre et de l'environnement de la University of Toronto accompagne sa classe lors d'une excursion à High Park. Ensuite, le professeur leur donne un échantillon de sol prélevé au fond de l'étang Grenadier et leur demande de rédiger un article sur les sédiments, en les reliant à des événements de l'histoire de Toronto. L'étudiant a été déconcerté : les données sédimentaires ne semblaient pas s'aligner sur les données historiques. À environ 25 centimètres du sommet de l'échantillon, il a vu ce qui semblait être une couche de goudron noir, qu'il a daté du début des années 1970. Mais quelle en est la cause ?

Il consulte les bases de données de l'université dans l'espoir de découvrir un événement régional — un incendie, par exemple, ou un grand projet de construction — qui pourrait expliquer le changement sédimentaire, mais il ne trouve rien. En désespoir de cause, il rédige une description de l'échantillon du sol et demande à ChatGPT de l'interpréter. Le robot répond en quelques secondes et établit un lien entre le goudron de l'échantillon et la construction de l'autoroute Queensway dans les années 1950.

Au début, l'étudiant trouve la solution absurde — la chronologie est insensée — mais il se rend vite compte qu'elle est correcte. Dans son analyse initiale, il avait mal daté l'échantillon de sol, attribuant les sédiments au développement de la construction d'après-guerre à des événements survenus 20 ans plus tard. ChatGPT avait corrigé cette erreur.

<https://torontolife.com/deep-dives/chatgpt-ai-cheating-revolutionizing-university-education/>



Quel autre outil numérique l'étudiant a-t-il utilisé en plus de ChatGPT ?

---

Qu'est-ce que l'étudiant a écrit dans ChatGPT ?

---

Quelle erreur ChatGPT a-t-il corrigée ?

---

---

Croyez-vous que l'étudiant ait triché ou qu'il a utilisé ChatGPT de manière éthique ? Justifiez votre réponse. (Les réponses peuvent varier)

---

---

#### TRICHERIE OU TECHNOLOGIE INTELLIGENTE ?

- 1960 : Apparition des calculatrices portables ; les écoles s'inquiètent des risques de tricherie.
- 1970 : On encourage l'utilisation de calculatrices en classe pour les mathématiques de base.
- 2001 : Création de Wikipédia ; les écoles s'inquiètent des risques de tricherie.
- 2010 : Wikipédia est un excellent point de départ.
- 2022 : Création de ChatGPT ; les écoles s'inquiètent des risques de tricherie.
- Aujourd'hui : Bien qu'il soit encore très tôt dans le développement et l'intégration de l'IA, il semble probable qu'elle devienne une partie acceptée de la façon dont les apprenants à tous les niveaux mènent des recherches et entreprennent des travaux. Il est possible que l'on encourage l'utilisation éthique de la technologie plutôt que de la restreindre.



## LES AVANTAGES DE L'AUTOMATISATION ET DE L'IA DANS LES MÉTIERS

L'automatisation est l'utilisation de la technologie pour effectuer des tâches sans intervention humaine. Il peut s'agir de machines simples, comme des tapis roulants, ou de robots complexes et de systèmes informatiques capables d'effectuer un large éventail de tâches de manière répétée. Les travailleurs installent des machines pour qu'elles répètent les mêmes tâches à l'aide d'un système d'automatisation. Cependant, ces machines ne peuvent rien faire d'autre.

En y ajoutant l'IA, les humains peuvent programmer ces machines de manière qu'elles détectent quand les choses vont mal, trouvent comment les réparer, apprennent de ces expériences, améliorent leur fonction et rapportent les changements aux humains. L'IA peut améliorer l'automatisation lorsque les deux travaillent ensemble. Lorsque c'est le cas, les avantages sont considérables. Par exemple, deux des principaux inconvénients de l'automatisation sont que les machines ne peuvent pas gérer des tâches complexes ou corriger les erreurs. L'ajout de capacités en matière d'IA et d'algorithmes programmés sur mesure permet de créer une technologie capable de prendre des décisions et de corriger les erreurs.



La robotique est un exemple de l'utilisation de l'IA dans les métiers. La robotique est une division des sciences et de l'ingénierie qui conçoit, développe, fabrique et exploite des robots. Ces robots sont des machines intelligentes conçues pour effectuer différents types de tâches. Les robots peuvent avoir différentes formes et tailles, et leur niveau d'intelligence et de sophistication varie.

Il ne fait aucun doute que l'IA a un impact significatif sur la façon dont le travail des ouvriers qualifiés est effectué. À mesure que l'IA est utilisée pour un plus grand nombre de tâches, nombreux sont ceux qui se demandent si elle ne va pas remplacer ces travailleurs. La possibilité que les travailleurs soient remplacés par des machines n'est pas une idée nouvelle. L'automatisation fait partie des processus de production et de fabrication depuis la première révolution industrielle. Le travail des ouvriers qualifiés a été modifié par l'automatisation, mais ils sont toujours très recherchés.

Des chercheurs de l'Organisation de coopération économique (OCDE) ont sondé 14 grandes confédérations syndicales à travers les pays de l'OCDE pour mieux comprendre ce que pensent actuellement les entreprises de l'avenir de l'IA dans leurs milieux de travail.



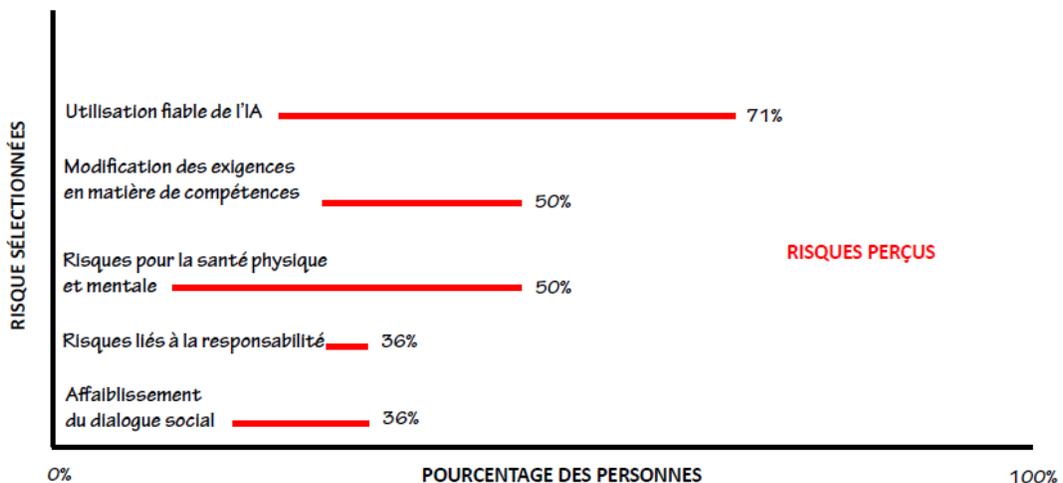
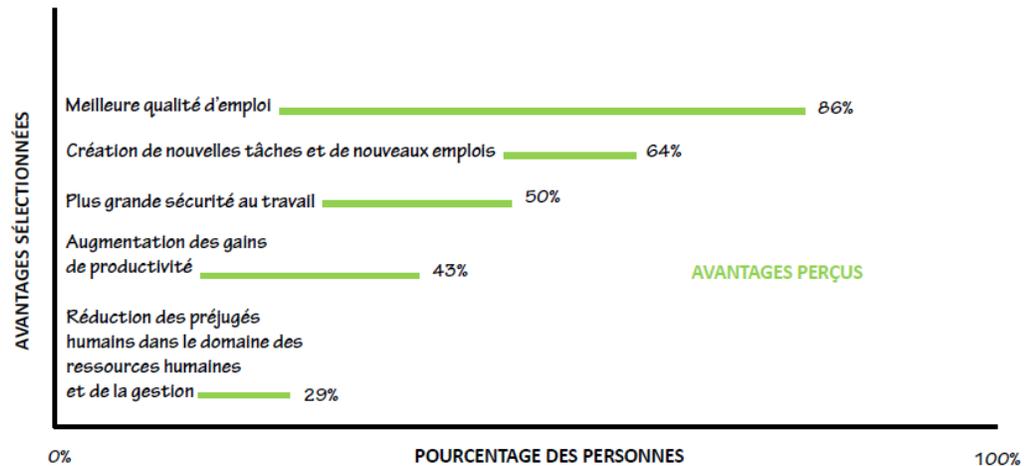
Comme l'on peut voir sur les graphique, une majorité de répondants a déclaré que l'adoption de l'IA pourrait améliorer la qualité du travail pour les travailleurs — peut-être grâce à une collaboration efficace entre les travailleurs et l'IA.

Cela pourrait se traduire par une réduction du temps de travail pour accomplir une tâche,

permettant une concentration plus importante sur des tâches plus intéressantes et une autonomie de travail accrue. Parallèlement, les données de l'enquête ont montré que de nombreux travailleurs de la sphère syndicale considèrent que l'IA crée de nouvelles tâches et de nouveaux emplois, tels que les rôles d'analystes de données, d'ingénieurs informaticiens, de scientifiques et d'experts en réseau.

## AI DANS DIFFÉRENTS MÉTIERS

L'IA crée de nouveaux emplois et modernise les métiers traditionnels en introduisant des technologies et des machines à la fine pointe du progrès. Grâce à l'amélioration de la technologie, il devient plus facile, plus aisé et plus rapide d'accomplir certaines tâches. L'IA peut suggérer les meilleurs processus et produits pour effectuer un travail et soulager les gens d'un travail qui pourrait être trop pénible pour être sécuritaire pour quelqu'un, comme soulever des machines lourdes. Elle peut également faciliter les travaux d'entretien en montrant aux travailleurs les zones problématiques précises, de sorte qu'ils n'aient pas à déconstruire un appareil entier.





Voici quelques exemples de l'IA effectuant le travail d'ouvriers qualifiés :

## Fabrication

- Airbus a développé un système d'IA pour analyser les données de performance des avions afin de prédire quand les pièces pourraient avoir besoin d'être remplacées ou entretenues, augmentant ainsi la sécurité, et réduisant les coûts d'entretien.

## Agriculture

- John Deere, fabricant de matériel agricole, utilise l'IA et l'apprentissage automatique pour analyser des échantillons de sol et d'autres données afin d'aider les agriculteurs à prendre de meilleures décisions au sujet du moment et de l'endroit où planter les cultures, ce qui permet un meilleur rendement des récoltes.

## Construction :

- Dans le secteur de la construction, l'IA est déjà utilisée pour automatiser des tâches telles que l'arpentage, la planification et la gestion de projet, ce qui permet d'améliorer l'efficacité et de réduire les coûts.

## Robots d'entrepôt

- Voici un exemple célèbre de collaboration entre l'homme et le robot : les robots dans les entrepôts d'Amazon travaillent aux côtés du personnel dans ses centres de traitement des commandes. Ces robots n'ont qu'une seule tâche : apporter les articles aux préparateurs de commandes afin qu'ils puissent les emballer et les étiqueter afin de les expédier. Pour ce faire, ils déplacent des étagères entières et sont programmés pour surveiller les humains afin d'éviter les collisions et les accidents. Alors que les robots existants sont limités à certaines zones, un nouveau modèle actuellement à l'essai, surnommé « Bert », sera capable de se déplacer en toute sécurité n'importe où sur le plancher de l'usine.

- 1.** Répondez aux 3 questions ci-dessous.  
( *Compétences numériques, niveau intermédiaire* )

Quelle est la différence la plus importante entre l'automatisation et l'IA ?

---

À l'aide des informations contenues dans l'article, décrivez un avantage de l'utilisation de l'IA dans chacun des secteurs énumérés.

- Fabrication : \_\_\_\_\_
- Construction : \_\_\_\_\_



- Agriculture : \_\_\_\_\_

Que pourra faire le nouveau robot d'entrepôt que les robots actuels ne peuvent pas faire ?

---

2.

Les avantages et les risques de l'IA perçus dans le lieu de travail identifiés dans l'étude de l'OCDE sont énumérés ci-dessous. Y a-t-il d'autres avantages ou risques que vous voulez inclure ? Inscrivez-les dans les espaces prévus à cet effet. Ensuite, classez les avantages et les risques dans l'ordre dans lequel vous pensez qu'ils auront le plus d'impact. (1 = le plus important).

(*Compétences numériques, niveau intermédiaire*) Les réponses peuvent varier.

Avantages	Ordre — n°
Meilleure qualité d'emploi	
Création de nouvelles tâches et de nouveaux emplois	
Plus grande sécurité au travail	
Augmentation des gains de productivité	
Réduction des préjugés humains dans le domaine des ressources humaines et de la gestion	

RISQUES	Ordre — n°
Utilisation fiable de l'IA	
Modification des exigences en matière de compétences	
Risques pour la santé physique et mentale	



Risques liés à la responsabilité	
Affaiblissement du dialogue social	





## 6. LA SANTÉ NUMÉRIQUE

---

### NOTE :

*Cette séance de formation a pour but de décrire à la manière dont les modes d'accès à l'information numérique à l'école, au travail ou dans la communauté peuvent avoir un impact sur votre santé physique et mentale et à vous faire réfléchir à ce sujet.*

*Certains impacts du numérique sur la santé, en particulier sur la santé mentale, sont très personnels et très complexes. Dans ces cas, vous avez besoin de plus que les informations présentées lors de cette séance de formation ; vous avez besoin d'amis et d'adultes de confiance, y compris des professionnels peut-être, pour vous aider à faire la part des choses.*

---



Si vous avez suivi la séance de formation sur les mots de passe et la sécurité, vous aurez lu des articles sur l'hygiène numérique. Les notions d'hygiène et de santé sont similaires, mais lorsque cette séance de formation parle de votre santé numérique, il s'agit de votre santé physique et mentale.

La révolution numérique a tout changé. Elle rend beaucoup de choses plus faciles et plus créatives, mais nous devons aussi réfléchir à l'impact de l'utilisation des outils numériques non seulement sur notre mode de vie et de travail, mais aussi sur notre santé et notre état d'esprit.

Le monde numérique fournit également une quantité infinie d'informations relatives à la santé. Et, comme pour tous les autres aspects de la transformation numérique, il est important de savoir comment l'utiliser en toute sécurité.

## **DR GOOGLE. J'APPELLE LE DR GOOGLE.**

Le terme « Dr Google » est apparu au début des années 2000, lorsque les gens ont commencé à utiliser le puissant moteur de recherche pour effectuer un autodiagnostic. En 2013, selon *The Conversation*, plus de la moitié des Canadiens interrogés ont déclaré utiliser le moteur de recherche Google pour effectuer un autodiagnostic. En 2020, 69 % des Canadiens ont utilisé Internet pour rechercher des informations sur la santé, et 25 % ont utilisé des sources en ligne pour faire un suivi de leur forme physique ou de leur santé. Les soins médicaux virtuels, l'autosurveillance et l'autodiagnostic en ligne sont devenus encore plus courants pendant la pandémie de la Covid.



La possibilité de chercher par soi-même des informations relatives à la santé peut être valorisante. Si vous n'avez pas facilement accès aux soins de santé ou si vous ne vous sentez pas écouté, le fait de pouvoir rassembler vos propres informations peut vous donner de l'assurance ; toutefois, il est généralement nécessaire d'en discuter avec un professionnel de la santé. Voici quelques-uns des problèmes liés à l'autodiagnostic :

- l'exagération des symptômes et l'absence du problème réel ;
- des retards dans la mise en œuvre du traitement nécessaire ;
- une augmentation du stress, de l'anxiété et de la dépression ;
- l'autodiagnostic entraîne souvent de moins bons résultats.

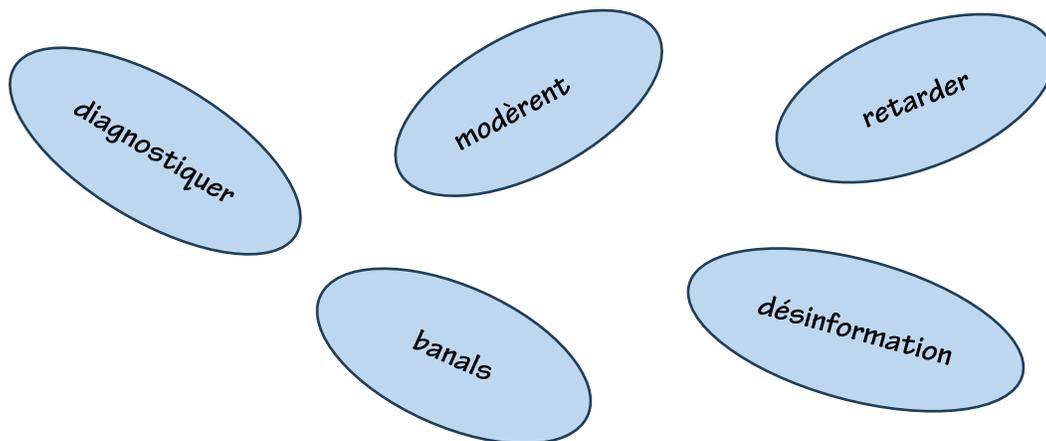
**1.**

Lisez l'article intitulé « Limiter les risques de l'autodiagnostic ». Il porte sur les inconvénients possibles de l'utilisation d'Internet pour obtenir des informations sur la santé. Par la suite, utilisez les mots figurant dans les bulles pour compléter les affirmations.

*(Compétences numériques, niveau intermédiaire)*



1. Cherchez des sites Web que \_\_\_\_\_ des agences de la santé ou gouvernementales.
2. Un mauvais diagnostic peut \_\_\_\_\_ l'obtention du bon traitement.
3. Plusieurs maladies graves peuvent avoir des symptômes \_\_\_\_\_.
4. La \_\_\_\_\_ est un problème commun lorsque l'on trouve des informations en lien avec votre santé sur les médias sociaux.
5. N'utilisez les sites Web que pour \_\_\_\_\_ les maladies bénignes.



## LIMITER LES RISQUES DE L'AUTODIAGNOSTIC

Les maladies que les moteurs de recherche diagnostiquent le mieux sont les maladies bénignes comme le rhume ou la grippe. Bien qu'il soit important que vous soyez informé en tant que patient, et qu'il existe des cas où des personnes souffrant de maladies mystérieuses ont trouvé des solutions sur Internet, l'utilisation de Dr Google pour établir un autodiagnostic comporte également des risques.

L'utilisation d'Internet pour s'autodiagnostic peut conduire à une erreur de diagnostic et retarder le bon diagnostic. De nombreuses maladies graves ont aussi des symptômes banals. Par exemple, les douleurs d'estomac peuvent être causées par des problèmes liés à l'estomac, à l'appendice, à la vésicule biliaire, à la rate, à l'intestin, au foie et à des problèmes gynécologiques. Il se peut aussi que vous ayez tout simplement trop mangé. Lors d'un autodiagnostic, il est facile de penser qu'il y a quelque chose de grave et de devenir anxieux. Au lieu de se contenter de recherches générales sur le Web, il est préférable d'utiliser des sites plus fiables que modèrent les facultés de médecine, les agences gouvernementales de santé et les organismes spécialisés dans les maladies, comme la Société canadienne du cancer, qui sont animés par des professionnels de la santé.



Même lorsque l'on utilise des sites fiables, il est possible de s'enfoncer dans le pays des merveilles de la « cyberchondrie ». Plus vous consultez de sites Web consultés, plus vous risquez que cela se produise. Les forums, les clavardages non modérés et les médias sociaux peuvent contenir des expériences personnelles qui ont mal tourné ou qui sont incomplètes, ce qui peut augmenter votre anxiété. On peut trouver de tout sur le Web et il peut être difficile de distinguer la réalité de la fiction.

Que le diagnostic soit correct ou incorrect, se traiter soi-même peut avoir des conséquences indésirables. Si vous avez de la chance, la seule conséquence sera une perte de temps et d'argent pour un traitement inefficace. Dans le cas contraire, le traitement pourrait aggraver votre état ou entraîner des complications ou des effets secondaires importants.

L'autodiagnostic numérique présente un autre risque : « l'empreinte » que vous laissez chaque fois que vous visitez un site Web. De nombreux sites peu fiables utilisent des outils pour suivre les visiteurs sur leurs sites Web. Vos données personnelles et les informations médicales que vous avez fournies volontairement peuvent être collectées, ou même vendues. Vous pouvez limiter ce risque en ne vous « abonnant » jamais à un site et en n'y inscrivant jamais d'informations personnelles.

## 2.

Pour chacun des risques énumérés dans le tableau, identifiez au moins une action que vous pouvez entreprendre pour réduire le risque.

*(Compétences numériques, niveau intermédiaire)*

RISQUE	ACTION
Suivre des instructions inexactes	
Perdre des informations personnelles	
Augmenter votre niveau d'anxiété	
Retarder l'obtention des soins médicaux dont vous avez besoin	
Perdre du temps et de l'argent sur de faux remèdes	



## PARLONS DES ASPECTS PHYSIQUES

La surutilisation de la technologie numérique peut avoir plusieurs effets négatifs sur la santé physique. Il s'agit ici de douleurs à la tête, au cou et au dos, de la santé des yeux et de l'ouïe, ainsi que d'un mauvais sommeil, de l'obésité et d'une tendance à ne pas faire d'exercice. Heureusement, il existe des précautions à prendre pour réduire, ou même prévenir, ces effets.

Regarder un appareil électronique pendant de longues périodes peut causer des douleurs au cou et au dos, ainsi qu'aux coudes, aux poignets et aux mains. De plus, l'utilisation d'ordinateurs portables et de téléphones intelligents peut faire en sorte que les personnes sont assises dans une mauvaise position du corps, c'est-à-dire selon une mauvaise fonction ergonomique. En plus des douleurs au dos dues à l'utilisation de l'ordinateur, souvent causées par une mauvaise posture pour jouer ou travailler à l'ordinateur, on signale des cas de « coude d'égoportrait (selfie) » ou de « pouce texto », causés par une utilisation excessive de la technologie. Les douleurs dans ces parties du corps sont appelées douleurs musculosquelettiques (se rapportant aux muscles et aux os).



### Qu'est-ce que l'ergonomie ?

L'ergonomie se définit comme l'étude de l'être humain dans son environnement de travail. Plus précisément, un ergonomiste conçoit ou modifie le travail pour l'adapter au travailleur, et non l'inverse. L'objectif est d'éliminer l'inconfort et le risque de blessure liés au travail. Le terme vient des mots grecs ERGON (travail) + NOMOS (lois naturelles).

Conseils pour prévenir ou réduire les douleurs musculosquelettiques :

- Faites attention à votre posture lorsque vous utilisez différents appareils.
- Adoptez une bonne position assise devant l'ordinateur en veillant à faire la meilleure utilisation de votre bureau, de votre siège et de votre écran. La hauteur du siège doit être réglée de manière que vos genoux soient à 90° par rapport au sol lorsque vos pieds sont à plat sur le sol. Vos coudes doivent également être à 90° par rapport à votre corps. Votre dos doit être droit et toucher le dossier de la chaise.



- Au lieu de tenir votre téléphone sur vos genoux, vous pouvez minimiser les problèmes de cou en le tenant devant vous. Positionner l'appareil de manière qu'il soit devant votre visage et que votre tête repose bien sur vos épaules est une bonne position pour votre cou.
- Si le fait d'écrire avec vos pouces vous fait souffrir, essayez d'utiliser d'autres doigts pour écrire ou utilisez un stylet.
- Prévoyez de courtes pauses régulières. Réglez une minuterie toutes les 20 à 30 minutes pour vous lever, vous étirer et marcher quelques minutes. Cela contribuera non seulement à réduire les douleurs musculaires et la fatigue des yeux, mais aussi le stress.

La fatigue des yeux est l'un des symptômes les plus fréquents d'un usage excessif de l'écran. Les signes de la fatigue des yeux à cause du numérique comprennent la sécheresse des yeux, des rougeurs autour des yeux, des maux de tête, une vision floue et même des douleurs dans le cou et les épaules.

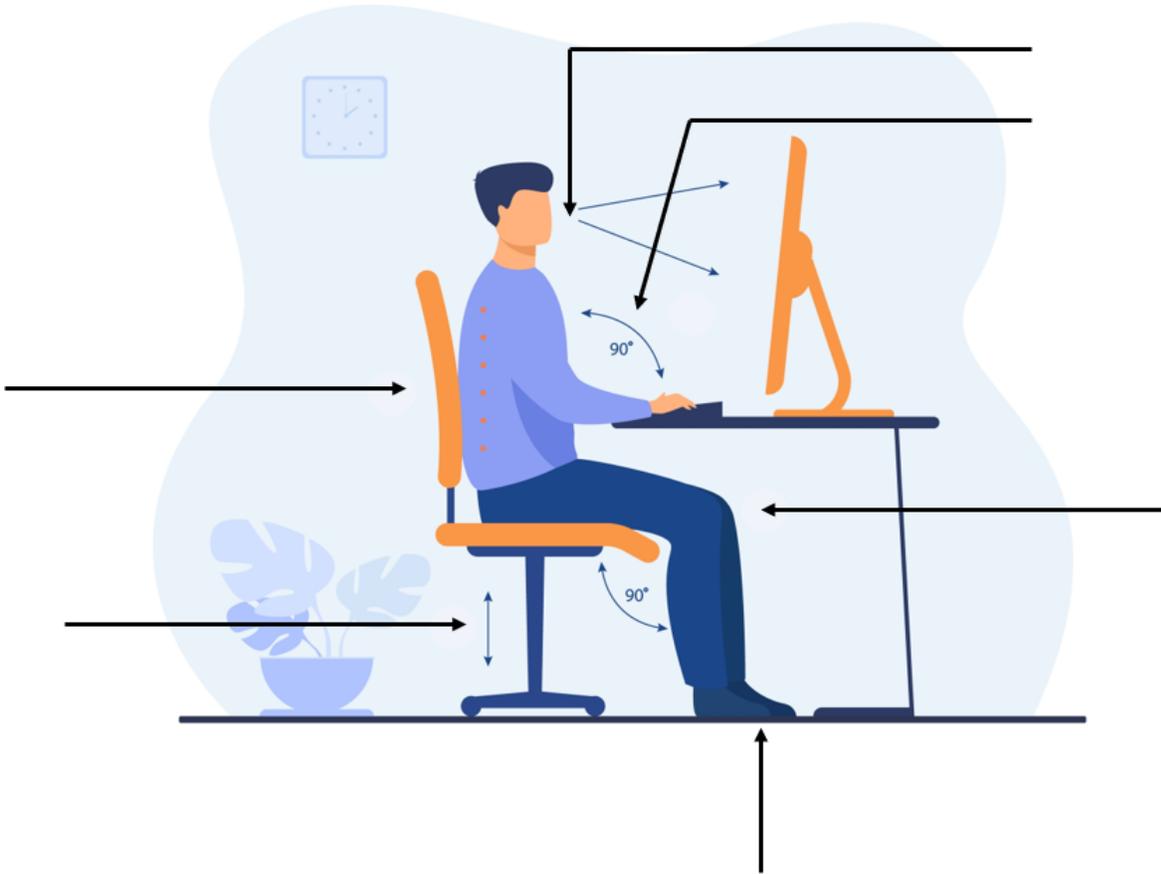
Conseils pour prévenir ou réduire la fatigue des yeux :

- Lorsque vous travaillez à un bureau, le haut de l'écran doit être à la hauteur de vos yeux et la distance entre vos yeux et l'écran doit être de 45 à 70 cm.
- Assurez-vous de cligner des yeux. En fait, lorsque nous fixons des appareils numériques, nous clignons moins souvent des yeux, ce qui assèche les yeux. Si la sécheresse des yeux vous gêne, des gouttes pour les yeux peuvent vous aider.
- Réduisez l'éclairage au-dessus de vous pour minimiser l'éblouissement causé par l'écran.
- Augmentez la taille du texte sur les appareils afin de pouvoir lire confortablement.

1.

Utilisez les informations de l'article « Parlons des aspects physiques » pour identifier les précautions ergonomiques prises par la personne pour prévenir les problèmes musculosquelettiques et de fatigue des yeux sur l'image.

(*Compétences numériques, niveau intermédiaire*)



La protection de l'ouïe est un autre élément important pour assurer votre santé numérique.

La perte de l'ouïe peut survenir lorsque l'on est souvent exposé à des sons forts. Selon l'Organisation mondiale de la santé, 1,1 milliard de jeunes dans le monde risquent d'endommager leur ouïe en écoutant de la musique trop fort au moyen d'un casque, d'écouteurs ou d'oreillettes.

Pensez-y d'un point de vue professionnel. Dans certains métiers spécialisés, votre travail vous oblige à être en contact avec des bruits forts générés par des machines. Sur ces chantiers, la protection auditive est un élément important et nécessaire de votre ÉPI (équipement de protection individuelle). Pensez à protéger votre ouïe de la même manière lorsque vous écoutez de la musique ou de la diffusion en continu.





Conseils pour prévenir ou réduire la perte de l'ouïe :

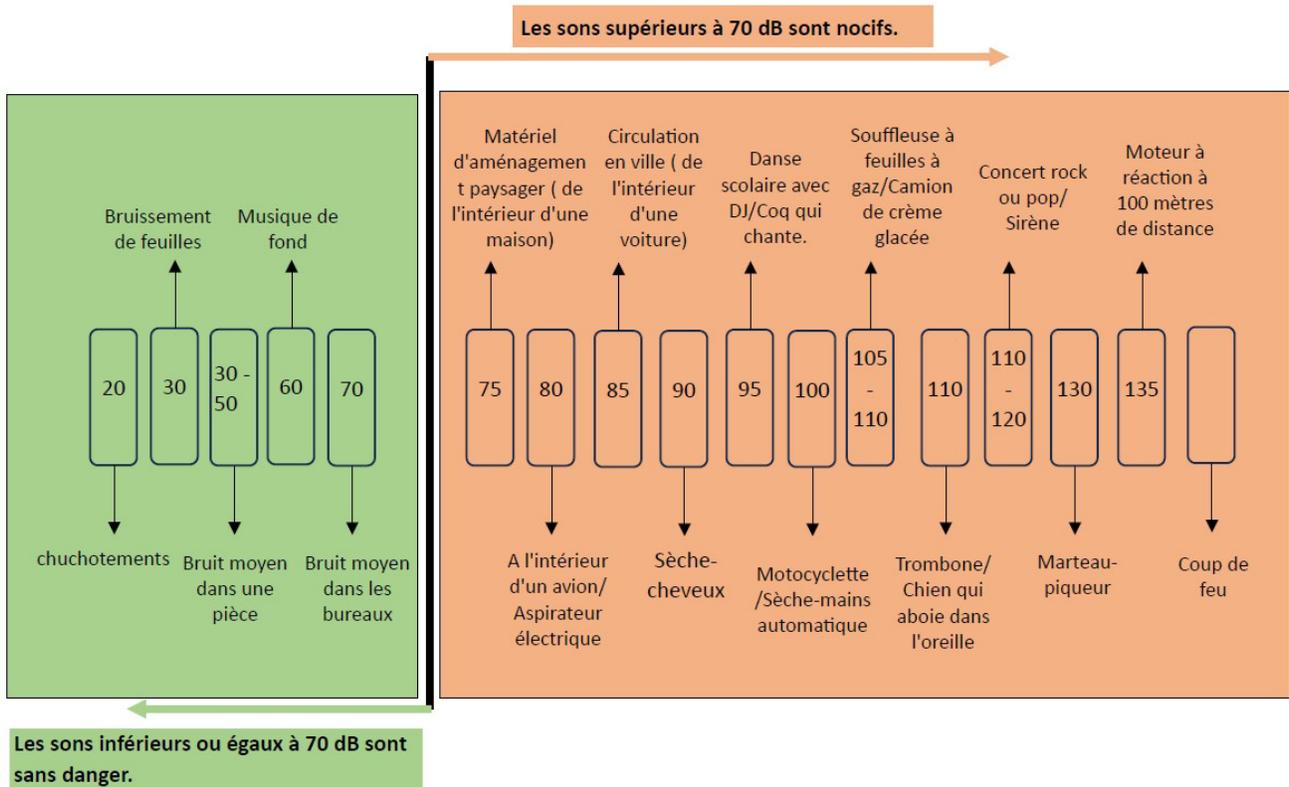
- Choisissez des écouteurs qui se placent à l'extérieur de l'oreille plutôt que des oreillettes qui se placent à l'intérieur de l'oreille. Cela permet d'avoir un espace supplémentaire qui contribue à protéger votre ouïe.
- Essayez de porter un casque antibruit, qui utilise des ondes spéciales pour bloquer les sons extérieurs.
- Les experts suggèrent qu'un son ne dépassant pas 85 décibels (dB) pendant 8 heures par jour est le « niveau sécuritaire » maximum pour l'exposition au bruit au travail.

Les décibels sont une unité de mesure du son. Leur abréviation est dB. Les sons inférieurs ou égaux à 70 dB sont considérés comme sans danger pour l'ouïe. Cela correspond au son d'une conversation normale entre deux personnes. Un bruit constant supérieur à 70 dB endommage l'ouïe au fil du temps.

## 2.

Utilisez les informations dans le diagramme des niveaux de bruit pour répondre aux questions.  
(Compétences numériques, niveau intermédiaire)

1. Quelle est la différence en décibels entre entendre du matériel d'aménagement paysager à l'extérieur ou à l'intérieur d'une maison ? \_\_\_\_\_
2. Prendre l'avion peut-il nuire à votre audition ? Encerclez votre réponse. OUI NON
3. Quel est le seuil de sécurité des sons ? \_\_\_\_\_
4. À combien de dB du niveau de sécurité se situe un sèche-cheveux ? \_\_\_\_\_
5. À part l'avion, quel est le bruit de transport le plus fort ? \_\_\_\_\_
6. Quelle est la différence en décibels entre un sèche-mains électrique et un sèche-cheveux ? \_\_\_\_\_



### Le sommeil

Dormir suffisamment est essentiel au bon fonctionnement de l'organisme. Vie saine Canada recommande de dormir de 8 à 10 heures par nuit jusqu'à l'âge de 17 ans et de 7 à 9 heures régulièrement entre 18 et 64 ans. On associe un sommeil de mauvaise qualité ou insuffisant à la dépression et à de nombreux problèmes de santé chroniques, y compris les maladies cardiaques, l'hypertension artérielle et l'obésité.



L'utilisation d'un ordinateur portable, d'une tablette ou d'un téléphone intelligent avant de se coucher peut faire en sorte qu'il est difficile de s'endormir. En effet, ces appareils émettent une lumière bleue qui peut vous empêcher de vous endormir et perturber votre rythme de sommeil. Certaines personnes pensent qu'elles ont besoin de leur écran pour se détendre (ce qui n'est pas vrai). Si c'est votre cas, faites quelque chose de passif comme écouter de la musique, lire un livre électronique ou regarder la télévision. Évitez les activités interactives comme les jeux vidéo ou le clavardage sur les médias sociaux. Les activités interactives peuvent davantage perturber votre sommeil que les activités passives.



Conseils pour encourager de bonnes habitudes de sommeil :

- Arrêtez d'utiliser votre téléphone intelligent, votre ordinateur portable et votre tablette au moins une heure avant de vous coucher. Lire un livre est plus susceptible de vous aider à vous détendre que de parcourir les médias sociaux.
- Le soir, rendez votre écran aussi sombre que possible. Certains lecteurs électroniques vous permettent de changer la couleur de l'écran et d'afficher des mots blancs sur fond noir. De nombreux appareils disposent également d'un « mode nuit », meilleur pour les yeux avant le coucher.
- Si vous le pouvez, ne laissez pas les écrans dans votre chambre à coucher.
- Créez une routine sans écran relaxante avant de vous coucher. Cela vous aidera à vous détendre avant de vous endormir.

## 3.

En plus de mieux gérer vos appareils numériques, il y a d'autres choses que vous pouvez faire pour améliorer la qualité de votre sommeil. Utilisez les informations que vous venez de lire et l'infographie de Santé publique Canada retrouvée à la page suivante, pour répondre aux questions. (*Compétences numériques, niveau intermédiaire*)

1. Quel pourcentage d'adultes de moins de 35 ans ne dort pas assez ? \_\_\_\_\_
2. Quel pourcentage des adultes a du mal à rester endormi ? \_\_\_\_\_
3. Quel pourcentage des adultes pourrait s'endormir au cours de la journée ? \_\_\_\_\_
4. Compte tenu de votre âge, combien d'heures devriez-vous dormir chaque nuit ? \_\_\_\_\_
5. Combien d'heures dormez-vous ? \_\_\_\_\_
6. Si vous dormez moins que le nombre d'heures recommandé, identifiez deux changements que vous pourriez apporter à vos habitudes de sommeil.

---

---

---

---



# LES ADULTES CANADIENS DORMENT-ILS SUFFISAMMENT?

Voici les recommandations<sup>1</sup> actuelles :



De 18 à 64 ans

**DE 7 À 9 HEURES**

de sommeil par nuit



De 65 ans et plus

**DE 7 À 8 HEURES**

de sommeil par nuit

**Mais...**

**1 adulte sur 4**  
âgé de **18 à 34 ans**

**1 adulte sur 3**  
âgé de **35 à 64 ans\***

**1 adulte sur 4**  
âgé de **65 à 79 ans**

**NE dort PAS**  
**suffisamment.**



\*Différence significative entre les hommes et les femmes

Parlons de la **qualité du sommeil**, d'accord?

**1 adulte sur 2**  
a de la difficulté à  
**s'endormir** ou à **rester endormi**.

**1 adulte sur 5**  
juge que son sommeil  
n'est pas réparateur.

**1 adulte sur 3**  
a de la difficulté à **demeurer éveillé**  
pendant les heures d'éveil.

Un certain nombre de facteurs sont liés à un **sommeil insuffisant** chez les adultes :



• **PLUS DE TEMPS DE SÉDENTARITÉ**

Les adultes qui ont un **sommeil insuffisant** révèlent une moyenne de **4,0 heures** de temps de sédentarité comparé à une moyenne de **3,5 heures** pour les adultes qui ont un **sommeil adéquat**.

• **LE STRESS CHRONIQUE**

**36,3 %** des adultes qui ont un **sommeil insuffisant** révèlent avoir un stress chronique comparé à **23,2 %** des adultes qui ont un **sommeil adéquat**.

• **UNE MAUVAISE SANTÉ MENTALE**

**12,3 %** des adultes qui ont un **sommeil insuffisant** révèlent avoir une mauvaise santé mentale comparé à **5,8 %** des adultes qui ont un **sommeil adéquat**.

Une bonne hygiène de sommeil pourrait procurer un meilleur sommeil<sup>2,3</sup>:

- évitez l'alcool, la caféine et la nicotine avant d'aller au lit
- couchez-vous et levez-vous à des heures régulières
- ayez recours à des techniques de détente et à des techniques de réduction du stress fondées sur la pleine conscience
- réduisez le bruit dans l'environnement de sommeil
- limitez les siestes à 30 minutes
- faites de l'exercice régulièrement
- passez en revue régulièrement vos médicaments avec votre médecin ou pharmacien





Source des données : Enquête canadienne sur les mesures de la santé (ECMS), 2014-2015.

<sup>1</sup> Hirshkowitz M, Whiton K, Albert SM, et coll. « National Sleep Foundation's updated sleep duration recommendations: Final report ». *Sleep Health* 2015; 1:233-43

<sup>2</sup> Irish LA, Kline CE, Gunn HE, Buysse DJ et Hall MH. « The role of sleep hygiene in promoting public health: A review of empirical evidence ». *Sleep Medicine Reviews* 2015; 22:23-36

<sup>3</sup> Suzuki K, Miyamoto M, Hirata K. Sleep disorders in the elderly: Diagnosis and management. *Journal of General and Family Medicine*. 2017 Apr;18(2):61-71

## UN BON SOMMEIL FAIT PARTIE D'UN MODE DE VIE SAIN.

POUR EN SAVOIR PLUS SUR LE SOMMEIL ET LA SANTÉ, CONSULTEZ [CANADA.CA](http://CANADA.CA)

### > CHERCHEZ

Activité physique, comportement sédentarité et sommeil

### > OBTENEZ DES DONNÉES

Indicateurs de l'APCSS



> SUIVEZ-NOUS SUR TWITTER : @GouvCanSante



> AIMEZ-NOUS

Sur la page Facebook des Canadiens en santé  
([www.facebook.com/CANenSante](http://www.facebook.com/CANenSante))

© Sa Majesté la Reine du chef du Canada, représentée par la ministre de la Santé, 2019. Cat. : HP35-92/1-2018F-PDF | ISBN : 978-0-660-27684-7 | Pub. : 180293



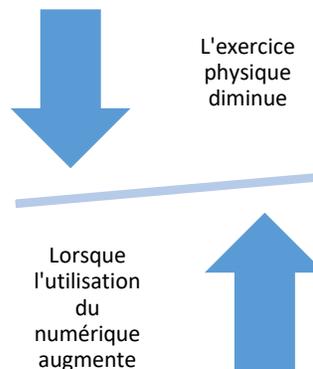
Agence de la santé  
publique du Canada

Public Health  
Agency of Canada

Canada

### Le manque d'exercice physique

La recherche confirme qu'il existe une corrélation entre la quantité de technologie numérique qu'utilisent les Canadiens et la quantité d'exercice physique qu'ils pratiquent. On parle de corrélation lorsqu'une chose a un impact direct sur une autre. La corrélation est donc la suivante :



Bien sûr, il y a des exceptions. De nombreuses personnes utilisent des applications numériques telles que des podomètres pour compter leurs pas ou faire un suivi des autres types d'exercices qu'elles effectuent. Ce suivi peut les encourager à augmenter la quantité d'activités sportives qu'elles pratiquent. De plus, certaines personnes utilisent des téléphones intelligents ou des dispositifs GPS pour pratiquer des activités physiques en plein air, comme la géocache.



Toutefois, plus nous utilisons nos appareils, moins nous sommes susceptibles de faire de l'exercice physique, et c'est un problème. Les adolescents et les jeunes adultes canadiens ont besoin d'un minimum de 60 minutes d'activité physique par jour pour atteindre et maintenir une bonne santé. Selon l'Organisation mondiale de la santé, seuls 3 élèves nord-américains sur 10 font cette quantité d'exercice.

- La marche rapide, le patinage, le vélo et le skateboard sont des exemples d'activité physique à intensité modérée.
- La course à pied, le basketball, le football et le ski de fond sont des exemples d'activités physiques à haute intensité.
- Les pompes, les redressements assis, l'haltérophilie et le fait de monter des escaliers et de faire du vélo sont des exemples d'activités de renforcement musculaire.
- Les activités de renforcement des os comprennent la course, la marche, le yoga et le saut à la corde.

4.

Remplissez l'autoévaluation suivante de Santé Canada pour évaluer votre niveau d'activité physique.

*(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier.*

Effectuez-vous ces activités ?	Oui	Pas encore
Vous faites de l'activité physique pendant 60 minutes par jour		
Si oui, que faites-vous ?		
Vous faites de l'activité physique à haute intensité 3 fois par semaine		
Si oui, que faites-vous ?		
Vous faites de l'activité physique axée sur le renforcement des muscles et des os 3 fois par semaine		
Si oui, que faites-vous ?		
Vous passez plus de 2 heures par jour en ligne (en dehors de l'école ou du travail)		
Si oui, comment pouvez-vous réduire ce nombre ?		



**5.**

Définissez dans vos propres mots les termes suivants trouvés dans cette séance de formation. (*Compétences numériques, niveau intermédiaire*)

Ergonomie :

---

---

Interaction :

---

---

Cyberchondrie :

---

---

Musculosquelettique :

---

---

Décibel :

---

---

Précautions :

---

---

Corrélation :

---

---

IPE :

---

---



## LA SANTÉ MENTALE, C'EST LA SANTÉ

On prend de plus en plus conscience que notre santé mentale mérite la même attention que notre santé physique. Une fois de plus, nous constatons que l'utilisation des outils numériques peut avoir des effets positifs et négatifs sur notre santé mentale, en fonction de la manière dont nous les utilisons et le montant de temps que nous leur consacrons.

Les outils numériques facilitent la communication avec la famille et les amis et nous permettent de nous sentir en contact avec des personnes, même celles que nous ne voyons pas souvent dans la vie réelle. Le fait d'être connecté permet aux gens de se sentir moins seuls ou isolés. La technologie numérique met également des informations à la disposition des personnes grâce à l'accès à Internet, ce qui leur permet de s'informer plus facilement sur la santé mentale et de chercher de l'aide.

Les médias sociaux ont également un impact particulièrement important sur la santé mentale. D'une part, ils peuvent favoriser les connexions, stimuler l'estime de soi et cultiver un sentiment d'appartenance. Mais ils peuvent aussi engendrer un stress considérable, créer une pression qui pousse les personnes à se comparer aux autres. Ils peuvent aussi contribuer à des sentiments de tristesse, d'isolement et même de dépression, et être un lieu propice à la cyberintimidation. Il est essentiel d'utiliser les médias sociaux avec précaution pour gérer leurs effets sur le bien-être mental.

La cyberintimidation existe bel et bien et c'est un problème grave.

Selon Sécurité publique Canada, 3 adolescents canadiens sur 10 affirment avoir été victimes d'intimidation en ligne. Si vous êtes victime de cyberintimidation, souvenez-vous que vous n'êtes pas seul et qu'il y a des choses que vous pouvez faire pour y mettre fin à cette situation et éviter qu'elle ne se produise à nouveau.

- Coupez le contact ; il est préférable de ne pas répondre.
- Protégez-vous ; utilisez les paramètres de confidentialité et changez souvent de mot de passe.
- Demandez de l'aide ; racontez ce qui s'est passé à une personne de confiance, qu'il s'agisse d'un parent, d'un enseignant ou d'un ami.

<https://www.canada.ca/en/public-safety-canada/campaigns/cyberbullying/cyberbullying-youth/what-to-do-if-you-re-being-cyberbullied.html>

### Qu'est-ce que la cyberintimidation ?

La cyberintimidation est l'utilisation d'ordinateurs, de téléphones intelligents ou d'autres appareils pour embarrasser, menacer ou blesser quelqu'un, se moquer de quelqu'un ou être méchant envers quelqu'un en ligne. Il s'agit d'un problème grave qui affecte les jeunes tous les jours.  
(Gouvernement du Canada)



## TROUVER UN ÉQUILIBRE

Comme nous le répétons sans cesse, les outils numériques ne sont ni « bons » ni « mauvais ». Ce qui compte, c'est la manière dont nous les utilisons. La clé pour gérer l'impact de la technologie sur la santé physique et mentale est de trouver un équilibre entre les avantages et les effets négatifs. Voici quelques conseils de *Citizen Advocates* (<https://citizenadvocates.net>) qui peuvent vous aider :

1. Fixez des limites. Limitez le temps passé devant un écran, en particulier avant de vous coucher, afin d'améliorer la qualité de votre sommeil.
2. Débranchez-vous. Faites régulièrement des pauses technologiques pour réduire votre stress et améliorer votre clarté mentale. Trouvez des activités que vous pouvez effectuer sans technologie, comme faire une promenade ou de la lecture.
3. Effectuer une utilisation réfléchie de la technologie. Soyez attentif à votre utilisation de celle-ci. Pensez à vous fixer des objectifs spécifiques pour gérer le temps que vous consacrez sur Internet, en ne consultant vos courriels ou les médias sociaux qu'à des heures déterminées, par exemple.
4. Recherchez les contacts en personne. Donnez la priorité aux interactions en personne avec vos amis, votre famille et vos collègues. Participez à des activités sociales qui ne nécessitent pas l'utilisation de la technologie.
5. Demandez de l'aide en cas de besoin. Si l'utilisation de la technologie a un impact sur votre santé mentale, demandez de l'aide à un professionnel de la santé mentale.

1.

Soulignez la meilleure solution d'un impact négatif d'une utilisation excessive de la technologie pour chaque exemple.

*(Compétences numériques, niveau intermédiaire)*

Ne pas pouvoir dormir	A. Faire une promenade matinale.
	B. Se déconnecter de toute technologie 30 minutes avant de se coucher.
Subir de la cyberintimidation	A. En parler à un adulte responsable.
	B. Les ignorer, ils finiront par s'arrêter.
Avoir des douleurs constantes au cou	A. Essayer de tenir son téléphone plus haut que ses genoux.
	B. Arrêter d'utiliser des écouteurs.
Vérifier constamment votre téléphone	A. Programmer de l'activité physique à votre horaire.
	B. Programmer des heures fixes pour consulter ses messages.
Se sentir isolé et déprimé	A. Parler à un ami ou à un conseiller en personne.
	B. Dire à un nouvel ami en ligne ce que vous ressentez.



## 2.

Faites la lecture de l'histoire de Juno, puis complétez le tableau pour identifier trois effets négatifs qu'elle subit et une solution possible pour chacun d'entre eux.  
*(Compétences numériques, niveau intermédiaire)*

Juno est une étudiante de 17 ans. Le jour, elle suit d'interminables cours en ligne, envoie des messages à ses amis et utilise des outils d'étude alimentés par l'IA. Le soir, elle se plonge dans le monde virtuel, participe à des événements en ligne et passe du temps avec ses amis dans des espaces virtuels. Bien que Juno semble s'épanouir dans ce mode de vie centré sur le numérique, derrière les écrans lumineux, elle éprouve des sentiments d'anxiété et de solitude, ainsi que la pression constante d'être toujours « dans le coup ». Elle publie des messages sur plusieurs plateformes plusieurs fois par jour et rafraichit constamment son téléphone pour s'assurer que son contenu est apprécié ou voir si elle a de nouveaux abonnés. Elle souffre constamment de douleurs au cou et au dos, ses yeux lui font mal et elle dort rarement bien. Elle panique lorsqu'il sa connexion Internet ne fonctionne pas bien et se sent triste lorsque son téléphone est silencieux. Elle fait défiler ses pages tard dans la nuit et garde son téléphone sous son oreiller lorsqu'elle s'endort enfin. Elle a du mal à rester saine d'esprit sans son téléphone.

IMPACT NÉGATIF	SOLUTION POTENTIELLE





# DÉVELOPPE TES COMPÉTENCES POUR RÉUSSIR

**DANS CETTE PARTIE DU CAHIER  
D'ACTIVITÉS, TU PEUX DONNER  
UN PETIT COUP DE POUCE À TES  
COMPÉTENCES EN REVISANT  
CERTAINES NOTIONS DE BASE DES  
COMPÉTENCES POUR RÉUSSIR.**

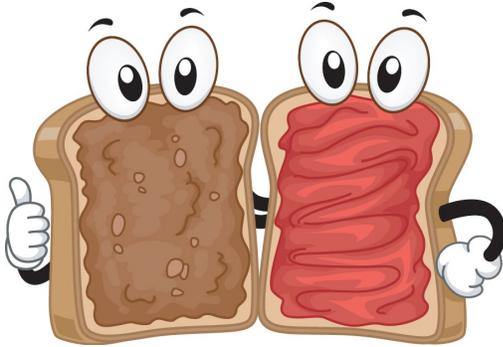
# COMPÉTENCES NUMÉRIQUES

Utilise la table des matières pour naviguer dans ce cahier d'activités. Suis ta progression en cochant chaque sujet terminé.

PARTIE ET SUJET		Page	√
AMPLIFICATEUR!		119	
1	Amplificateur de compétences numériques – vie privée en ligne et cybersécurité	121	
2	Amplificateur de compétences numériques – un court historique des mots de passe	125	



## 1. VIE PRIVÉE EN LIGNE ET CYBERSÉCURITÉ BEURRE D'ARACHIDES ET CONFITURE



Tout comme le beurre d'arachides et la confiture, la protection de la vie privée en ligne et la cybersécurité sont bonnes en soi, mais elles sont bien meilleures lorsqu'elles sont ensemble. Bien utilisées, les pratiques de protection de la vie privée et de sécurité sont très efficaces pour prévenir les intrusions de mauvais acteurs en ligne des particuliers et des entreprises.

La protection de la vie privée en ligne fait référence à votre droit et à votre responsabilité de contrôler la quantité d'informations qui sont vues, qui les voit et comment elles sont vues, lorsque vous êtes connecté à Internet.



La cybersécurité fait référence à la protection des données numériques stockées dans des appareils électroniques. Elle comprend l'utilisation des meilleures pratiques pour empêcher l'accès non autorisé aux données et la gestion des situations de manière à réduire les impacts d'un accès non autorisé.



## VIE PRIVÉE EN LIGNE

Les pratiques de protection de la vie privée en ligne protègent vos données personnelles dans la vie quotidienne et au travail contre les individus et les organismes qui veulent voler vos données à des fins criminelles.

Les données personnelles, également appelées informations personnelles ou informations personnellement identifiables, sont toutes les informations qui vous concernent directement.

## CYBERSÉCURITÉ

Les pratiques de cybersécurité protègent les données numériques contre les menaces externes commises sur Internet. Des pratiques de cybersécurité efficaces au sein des organismes permettent de préserver la sécurité des données personnelles.

Les données numériques sont des informations présentées électroniquement dans un format ou un langage que les machines peuvent lire et comprendre.



## EXEMPLES DE CYBERATTAQUES ET DE VIOLATIONS DE DONNÉES COURANTES

- Le vol d'identité, fraude, extorsion
- Les logiciels malveillants, l'hameçonnage, le pollupostage, le « spoofing », les logiciels d'espionnage, les chevaux de Troie et les virus
- Le matériel volé, tel que des ordinateurs portables ou des appareils mobiles
- Les attaques par déni de service (DdS)
- La recherche de mots de passe
- L'infiltration de système
- La dégradation de sites Web
- L'abus des messageries instantanées
- Le vol de propriété intellectuelle (IP)

Il existe de nombreuses façons de protéger votre vie privée en ligne dans la vie quotidienne et au travail, et de nombreuses façons pour les particuliers comme vous et pour les organismes et entreprises de prévenir les attaques en matière de cybersécurité. Certaines des pratiques les plus utiles sont décrites dans les listes de conseils qui suivent.



## **LES MEILLEURES PRATIQUES À UTILISER POUR PRÉVENIR LES VIOLATIONS DES DONNÉES À CARACTÈRE PERSONNEL**

- Utilisez toujours des mots de passe robustes.
- Utilisez l'authentification multifactorielle (AMF) dans la mesure du possible.
- Ne partagez jamais vos mots de passe ou vos identifiants de connexion.
- Veillez à ce que vos comptes de médias sociaux contiennent très peu d'informations personnelles identifiables.
- Utilisez un logiciel antivirus.
- Vérifiez la sécurité des sites Web avant d'y accéder. Par exemple, l'adresse commence-t-elle par https (sécurisé) ou http (non sécurisé) ?
- Désactivez le suivi sur les appareils mobiles. Cela augmente votre niveau de confidentialité, et vous verrez moins de publicités personnalisées et de suggestions de recherche.
- N'ouvrez pas ou ne cliquez pas sur des liens dans des textes ou des courriels provenant de sources que vous ne reconnaissez pas.
- Choisissez des environnements de confidentialité plus stricts lorsque l'option existe sur un site Web.
- Vérifiez les adresses de texte ou de courriel avant d'envoyer des messages ou des pièces jointes contenant des données personnelles afin d'éviter tout envoi accidentel à la mauvaise personne ou au mauvais organisme.
- Ne laissez jamais de documents personnels privés, ou de documents contrôlés par votre employeur, visibles sur l'écran d'un ordinateur. Ils peuvent être copiés, lus ou photographiés par des personnes non autorisées.



## **LES MEILLEURES PRATIQUES QUE VOTRE EMPLOYEUR PEUT UTILISER POUR PRÉVENIR LES FAILLES DE CYBERSÉCURITÉ**

- Disposer d'une politique de cybersécurité
- Maintenir les logiciels et le matériel informatique à jour
- Installer un logiciel antivirus et un logiciel contre les programmes malveillants sur tous les ordinateurs
- Maintenir à jour les logiciels antivirus et anti-programmes malveillants
- Exiger une authentification multifactorielle (AMF).
- Fournir aux employés une formation sur la protection de la vie privée et la sécurité.
- Tester régulièrement les employés en leur envoyant de faux courriels d'attaque.



- *Gérer l'accès aux données afin que seules les personnes qui en ont besoin puissent les consulter.*
- *Ne pas conserver pas plus de données que nécessaires*
- *Sauvegarder régulièrement les données.*
- *Crypter toutes les données, y compris les courriels.*
- *Disposer d'un plan d'intervention en cas de cyberattaque et le mettre à jour régulièrement*



## 2. UN COURT HISTORIQUE DES MOTS DE PASSE

L'histoire nous apprend que les mots de passe — sous forme de codes, de mots de passe ou de phrases de passe parlés — sont utilisés depuis des milliers d'années pour accéder à un lieu, à un groupe ou à un objet. La plupart des mots de passe parlés changeaient fréquemment afin que les informations, les objets ou les lieux qu'ils protégeaient soient conservés en toute sécurité.

Aujourd'hui, l'évolution rapide de la technologie rend encore plus importante l'utilisation de mots de passe et de systèmes de mots de passe mis à jour et régulièrement modifiés. Vous devez évoluer en même temps que la technologie. Plus vous prenez du retard, plus vous vous exposez à une tentative de vol d'identité ou à une grave atteinte à la protection de vos données.



S'il est intéressant de regarder en arrière et de voir comment nous en sommes arrivés là, la chose la plus importante à retenir est de continuer à regarder vers l'avant.



### AVANT LES ORDINATEURS

Les mots de passe parlés existent depuis que le langage parlé existe. Si vous ne connaissiez pas le mot de passe ou le mot secret, vous n'aviez pas le droit d'y accéder. Voici quelques exemples :

« Sésame ouvre-toi ! » (dans 1001 nuits de Galland)

« Vive le roi ! » (dans Hamlet de Shakespeare)

Les « mots d'ordre » utilisés par les armées dans la Rome antique et changés quotidiennement.

Le premier exemple de système d'identification biométrique (spécifique à certaines parties du corps d'une personne) remonte à la fin des années 1800 à Paris, en France. Alphonse Bertillon a mis au point une méthode permettant de prendre et d'enregistrer des mesures du corps spécifiques afin de classer et de comparer les criminels.

La prise d'empreintes digitales a suivi dans les années 1880 et a été utilisée à la fois pour identifier les criminels et comme forme de signature légale pour les contrats.



## APRÈS LES ORDINATEURS

Aujourd'hui, les mots de passe numériques, les phrases de passe et d'autres formes d'informations personnelles uniques ont évolué pour faire les mêmes choses que les premières formes parlées et physiques.

### L'ÉVOLUTION DES MOTS DE PASSE

Mots de passe	La première utilisation connue d'un mot de passe numérique a eu lieu au MIT (Massachusetts Institute of Technology) en 1961. Les mots de passe de base se résumaient généralement à un mot. Les organisations ont ensuite commencé à ajouter un chiffre, puis des caractères spéciaux et des lettres majuscules.
Phrases de passe	Une phrase de passe est un mot de passe composé d'une phrase ou d'une combinaison de mots, de préférence avec des caractères spéciaux et des chiffres pour le rendre plus complexe. Une phrase de passe longue ou construite de manière aléatoire est beaucoup plus longue à déchiffrer qu'un simple mot de passe. Par exemple, le site Web BetterBuys estime qu'il faudrait plus de dix ans pour craquer un mot de passe construit de manière aléatoire comme j9@vAg7 \$.
Gestionnaire de mots de passe	Un gestionnaire de mots de passe n'est pas une personne. Il s'agit d'un outil numérique qui stocke et récupère tous vos mots de passe dans un coffre-fort crypté qui ne peut être ouvert que par votre mot de passe principal, qui fait office de clé de décryptage. Sans cette clé, vos autres mots de passe restent cryptés et à l'abri des pirates. Les gestionnaires de mots de passe sont accessibles en ligne via une plateforme Web ou sur vos appareils mobiles via une application.
AMF	Introduite au début des années 2010, l'AMF, ou authentification multifactorielle est un processus qui ajoute une couche supplémentaire de sécurité à vos appareils et comptes ou à ceux de votre employeur. L'authentification de votre droit d'accès est validée par l'utilisation d'une combinaison de différents facteurs, y compris quelque chose que vous connaissez (par exemple, un mot de passe), quelque chose que vous avez



(par exemple, un jeton physique), ou quelque chose que vous êtes (un élément biométrique). L'AMF nécessite à la fois un mot de passe et une ou plusieurs vérifications supplémentaires pour accéder à vos appareils ou à vos comptes. L'identification à deux facteurs est un type d'AMF.

Les dates importantes de l'accès numérique biométrique (accès utilisant des parties du corps) sont les suivantes :

1980 : le National Institute of Standards and Technology (Institut national des normes et de la technologie) crée un groupe sur la reconnaissance vocale chargé d'étudier et de faire progresser les processus de la technologie de la reconnaissance vocale.

Biométrie  
numérique

1991 : Première utilisation de la technologie de détection faciale rendant possible la reconnaissance en temps réel.

1994 : Le premier algorithme de reconnaissance de l'iris est breveté.

2013 : Apple a inclus l'identification par empreinte digitale pour déverrouiller l'iPhone, amorçant l'acceptation à grande échelle de la biométrie comme moyen d'authentification.

Aujourd'hui, la reconnaissance faciale et vocale, ainsi que les empreintes digitales sont les données biométriques les plus couramment utilisées pour fournir un accès numérique.

En ce qui concerne l'avenir, de nombreux experts en sécurité prédisent que ce que nous considérons aujourd'hui comme des mots de passe (combinaisons de lettres, de chiffres et de symboles) n'existera plus.





# RÉPONSES AUX EXERCICES

LES RÉPONSES DES EXERCICES DE  
COMPÉTENCES POUR RÉUSSIR

# COMPÉTENCES NUMÉRIQUES

Utilise la table des matières pour naviguer dans ce cahier d'activités. Suis ta progression en cochant chaque sujet terminé.

PARTIE ET SUJET		Page	√
RÉPONSES!		129	
0	Associations de tâches et de compétences	131	
1	Les métiers spécialisés se transforment grâce au numérique !	133	
2	Mots de passe et cybersécurité	139	
3	Gérer les médias sociaux avec intelligence	145	
4	Questions d'argent en ligne	149	
5	Utiliser l'IA	157	
6	La santé numérique	163	



## 0. ASSOCIATIONS DE TÂCHES ET DE COMPÉTENCES

**VÉRIFIE TES RÉPONSES CI-DESSOUS.**

Les réponses suggérées se trouvent ci-dessous. C'est possible que tu aies pensé à d'autres compétences essentielles qui s'appliquent aussi.



Tâche	Compétences utilisées
Trouver les informations nécessaires pour programmer un nouvel iPhone	L, CN, RP
Faire une demande de permis d'apprenti conducteur	L, Ré, RP
Acheter des billets pour un concert	CN, L, RP
Aider à organiser une collecte de fonds pour ton équipe sportive	Cal, RP, Com, Col, CI
Préparer un plan pour payer les bottes quand tu te rends compte qu'elles sont plus chères que prévu.	RP, Cal, L
Trouver un autre moyen de transport lorsque tu ne peux pas utiliser la voiture pour aller skier.	Com, Col, CI
Envoyer un texto à ton entraîneur pour lui dire que tu seras en retard à ton entraînement, lui expliquer pourquoi et comment tu vas rattraper ton retard	CN, Ré, RP, Col
Arriver de bonne heure au bureau pour apprendre à utiliser le nouveau système de paiement	Cal, Col, Com
Regarder les horaires des transports en commun pour arriver à l'heure à ton nouveau travail	RP, Cal, CN





## 1. LES MÉTIERS SPÉCIALISÉS SE TRANSFORMENT GRÂCE AU NUMÉRIQUE !

1.

À l'aide des informations contenues dans l'article portant sur les quatre révolutions industrielles, complétez le tableau afin de mieux comprendre les principaux changements survenus au cours de chacune des révolutions. Cochez le numéro de la révolution qui correspond à chaque affirmation. (*Compétences numériques, niveau intermédiaire*)

DESCRIPTEUR DE LA RÉVOLUTION INDUSTRIELLE	1 <sup>re</sup>	2 <sup>e</sup>	3 <sup>e</sup>	4 <sup>e</sup>
Également appelée l'ère de l'électricité		✓		
A considérablement modifié l'industrie textile	✓			
Également appelée l'ère numérique				✓
A commencé au milieu du 20 <sup>e</sup> siècle			✓	
L'économie est passée de l'agriculture à l'industrie	✓			
Début des chaînes d'assemblage		✓		
L'utilisation des ordinateurs a commencé			✓	
Les machines fonctionnent à l'aide de moteurs à l'eau ou à la vapeur	✓			
Évolution de la 3 <sup>e</sup> révolution				✓
Également appelée l'ère de l'information			✓	
Début de la production de masse		✓		
A eu lieu au cours des 18 <sup>e</sup> et 19 <sup>e</sup> siècles	✓			
L'impact sur les métiers se poursuit au 21 <sup>e</sup> siècle				✓
A considérablement modifié l'industrie du chemin de fer		✓		



Skills/Compétences Canada identifie les compétences numériques comme l'une des trois principales compétences pour réussir dont ont besoin les techniciens en réparation automobile et les mécaniciens d'entretien, reconnaissant que les véhicules d'aujourd'hui sont devenus des ordinateurs sur roues.

1.

Dans la colonne N° de tâche du tableau, inscrivez les numéros des tâches de travail qui correspondent aux outils numériques pour lesquels ils sont le plus souvent utilisés. L'une d'entre elles est déjà effectuée pour vous. (*Compétences numériques, niveau intermédiaire*)

Outil numérique	N° de tâche	Tâche au travail
Traitement de texte	5	1. Effectuer des relevés d'énergie électrique.
Logiciel de tableur	11	2. Effectuer des réparations complètes.
Logiciel de communication	8	3. Télécharger des données destinées à réguler les paramètres de fonctionnement d'un véhicule.
Logiciel de dessin	6	4. Accéder à des données telles que les codes d'erreur des ordinateurs de bord.
Bases de données	9	5. Rédiger des lettres aux courtiers d'assurance pour leur présenter les résultats des inspections mécaniques.
Internet	10	6. Utiliser le logiciel graphique intégré aux outils de balayage pour accéder aux affichages de données de l'oscilloscope, tels que les valeurs des signaux et les schémas d'allumage de l'oscilloscope.
Multimètre (peut mesurer plusieurs propriétés électriques)	1	7. Effectuer des relevés énergétiques et dépister les problèmes.
Équipement électronique	4	8. Échanger des courriels avec d'autres techniciens dans d'autres lieux.



Outils de balayage tels que les oscilloscopes (affichent des signaux électriques et montrent comment les signaux évoluent dans le temps)	7	9. Récupérer les informations sur les réparations et les dessins techniques.
Ordinateurs portables connectés à des modules de commande logique numérique (contrôleurs programmables qui permettent aux machines d'exécuter des processus sans intervention humaine)	3	10. Participer aux cours de formation et aux séminaires proposés par les fournisseurs et les employeurs.
Équipements informatisés tels que les machines de réglage de la trajectoire des roues	2	11. Enregistrer et suivre les heures facturables.

Source : <https://www.skillscompetencescanada.com/wp-content/uploads/2021/02/Automove-Service-PDF.pdf>

## DÉVELOPPEMENTS NUMÉRIQUES DANS LE DOMAINE DU SOUDAGE

1.

Complétez les affirmations suivantes à l'aide des informations contenues dans la chronologie.  
(*Compétences numériques, niveau intermédiaire*)

1. Le soudage à l'arc au carbone fonctionne à l'aide de générateurs électriques.
2. Le soudage de goujons a d'abord été utilisé dans les secteurs du transport maritime et de la construction.
3. Durant le processus de soudage à l'arc, l'arc se déplace entre deux électrodes de carbone.
4. Au cours des années 1930, on note plusieurs développements importants dans le domaine de la soudure ; la création de codes de soudage, le soudage de goujons et le soudage à l'arc submergé.
5. Le premier chalumeau pour le soudage a été conçu entre les années 1900 et 1930.
6. Le soudage à la thermité est utilisé pour souder les rails de chemin de fer.
7. Le soudage automatique est très utilisé dans l'industrie automobile.



## 2.

Soulignez les mots ou les phrases dans l'article portant sur les développements numériques dans le domaine du soudage pour répondre à toutes les questions ci-dessous.  
(*Compétences numériques, niveau intermédiaire*)

1. Quels sont les avantages de la RA ?
2. Pourquoi le soudage à l'arc avancé est-il si utile ?
3. Que peuvent faire les apprentis soudeurs lorsqu'ils utilisent la RV ?
4. Pourquoi la RA est-elle un outil de formation si précieux ?
5. Quelle est l'incidence de la RA sur les coûts et les risques ?
6. Qu'est-ce que le soudage robotisé ?
7. Quel est l'impact attendu de la quatrième révolution industrielle sur l'industrie manufacturière ?

### DÉVELOPPEMENTS NUMÉRIQUES DANS LE DOMAINE DU SOUDAGE

Comme le montre la chronologie de la page précédente, les outils utilisés pour le soudage ont considérablement évolué depuis les premiers outils manuels de base et le feu jusqu'à l'introduction de batteries, d'électrodes, de systèmes automatiques et, aujourd'hui, de développements numériques faisant appel à l'intelligence artificielle (IA). Parmi les développements numériques les plus récents, citons le soudage à l'arc avancé, la réalité augmentée (RA) et la réalité virtuelle (RV), ainsi que le soudage robotisé. Une brève description de chacun d'entre eux est présentée ci-dessous.

#### Soudage à l'arc avancé :

- Résiste à la corrosion, ce qui le rend parfait pour les opérations de soudage chimique, nucléaire et toxique.

#### Réalité augmentée (RA) et réalité virtuelle (RV) :

- La réalité augmentée rend la formation plus visuelle, plus attrayante et plus éducative. Elle permet également de réduire le coût des matériaux utilisés pour la formation, de modérer les risques et de permettre aux éducateurs de former plus de nouveaux soudeurs en même temps. La RA permet à l'utilisateur d'entrer dans un environnement réel, de toucher et de sentir un objet réel et d'« augmenter » cet objet en lui donnant une nouvelle forme, en modifiant son apparence de manière réaliste. Par exemple, grâce à la RA, un étudiant en soudage peut prendre une pièce en plastique et



interagir avec elle alors qu'elle se comporte comme une pièce en acier au carbone, en acier inoxydable ou en aluminium lorsqu'elle est soudée. C'est très proche de l'expérience de soudage réelle, de sorte que les stagiaires peuvent voir et ressentir un environnement de soudage réel en utilisant un véritable équipement de soudage, tels qu'un masque de soudage et des torches de soudage.



- La RV transporte l'utilisateur dans un monde entièrement généré par ordinateur où il peut faire semblant de souder. L'expérience ressemble à celle d'un jeu vidéo.

## Soudage robotisé :

- Relie les personnes, les machines et les technologies intelligentes. Il s'agit de machines équipées de technologie numérique, y compris l'IA, utilisées aux côtés de soudeurs humains hautement qualifiés. Le soudage robotisé n'a rien à voir avec un robot humanoïde utilisant un chalumeau. Il s'agit de la nécessité de faire progresser la technologie de l'industrie 4.0. La quatrième révolution industrielle changera la façon dont la production manufacturière est automatisée grâce à l'utilisation de technologies intelligentes.



Document édité et traduit. Source : <https://seaberyat.com/en/welding-technology-trends-2021-beyond/>





## 2. MOTS DE PASSE ET CYBERSÉCURITÉ

1.

Utilisez les informations contenues dans les conseils pour identifier ce qui ne va pas avec chacun de ces mots de passe. Mettez ensuite à jour chaque mot de passe pour le rendre plus fort. (*Compétences numériques, niveau intermédiaire*)

Mot de passe	Pourquoi est-il faible ?	Réécrire pour le rendre plus fort. Voici quelques exemples.
Abcde 3456789	<i>Il utilise des chiffres et des lettres dans l'ordre.</i>	djFyGi0496745 Assortiment aléatoire de chiffres et de lettres. Certaines sont en majuscules.
chatsattrapentsouris	<i>Il utilise des mots dans un ordre logique. Les phrases de passe doivent être composées d'au moins 4 mots et d'au moins 15 caractères.</i>	micecucUm_bersstacit Utilisation de mots qui ne sont pas habituellement associés à des chats orthographiés à l'envers à la fin. Ajout d'un trait de soulignement.
MmFd386QR990	<i>Il ne comprend aucun symbole.</i>	Mm_Fd38**6Q%R990 Ajout d'un trait de soulignement, d'un astérisque et d'un symbole de pourcentage



X31monmotdepassegh3\$	<i>Il utilise le mot « mot de passe ».</i>	X31nFiugSpodkg3\$ Utilisation de lettres aléatoires. Ajout de majuscules.
-----------------------	--	--

1.

Écrivez la signification de chacune des abréviations ou chacun des mots suivants.  
(*Compétences numériques, niveau de base*)

ABRÉVIATION OU MOT	SIGNIFICATION
NIP	<i>Numéro d'identification personnel</i>
TEXTO	<i>Service de messages courts</i>
AMF	<i>Authentification multifactorielle</i>
CODE	<i>Mot de passe à usage unique</i>

2.

L'authentification à plusieurs facteurs exige que vous établissiez un lien entre qui vous êtes, quelque chose que vous connaissez et quelque chose que vous possédez afin de fournir une couche supplémentaire de sécurité numérique.

Identifiez chaque facteur énuméré ci-dessous comme étant soit :

1. Qui vous êtes.
2. Ce que vous savez.
3. Ce que vous avez.

(*Compétences numériques, niveau intermédiaire*)



FACTEUR	N°
NIP	2
Lecteur d'empreintes digitales	1
Jeton matériel	3
Carte à puce	3
Questions de sécurité	2
Reconnaissance vocale	1
Texte	2
Numériseur d'iris	1
Authentificateurs basés sur des applications	3
Reconnaissance faciale	1
Mots de passe et phrases de passe	2

### 3.

Quand avez-vous eu besoin d'utiliser l'AMF ? Pour des opérations bancaires ? Pour le magasinage ? Au travail ? D'autres situations ? Citez jusqu'à trois de ces situations et décrivez les mesures que vous avez dû prendre dans chacune d'entre elles. Vous n'avez pas encore utilisé l'AMF ? Interrogez quelqu'un qui l'a fait.

*(Compétences numériques, niveau intermédiaire)*

Situation : OPÉRATIONS BANCAIRES

Étapes :

*Saisissez l'identifiant et le mot de passe.*

*Sélectionnez un courriel ou un message texte pour recevoir le code.*

*Saisir le code pour accéder au compte.*

Situation : Système informatique de l'employeur



Étapes :

Saisissez l'identifiant et le mot de passe.

Sélectionnez l'option courriel ou message texte pour recevoir votre code.

Saisir le code pour accéder au compte.

Note : Le mot de passe doit être modifié tous les 3 mois.

Situation : Site Web du gouvernement pour les informations fiscales personnelles

Étapes :

Saisir l'identifiant et le mot de passe.

Répondre à la question de sécurité.

Choisir de recevoir le code par texte ou par message vocal.

Saisir le code pour accéder au compte.

1.

Dans le scénario qui suit, Martin travaille depuis longtemps dans l'industrie manufacturière, mais il est un nouvel employé de DIGICAN, une entreprise manufacturière qui pratique un niveau élevé de sécurité numérique. C'est nouveau pour Martin et il a déjà du mal à accepter certaines pratiques. Martin rejette la faute sur la technologie et affirme que c'est le problème de l'employeur et non sa responsabilité. Lisez ce qui s'est passé lors de son premier jour et soulevez tout ce que vous pensez qu'il aurait pu faire différemment.

*(Compétences numériques, niveau intermédiaire)*

Le premier jour, Martin était impatient de connaître l'entreprise et il est arrivé en retard à la séance d'information sur la sécurité. Le temps qu'il arrive, le formateur avait une autre réunion et il a donc donné à Martin des instructions écrites et reporté la formation à trois jours plus tard. Martin a suivi les instructions pour se connecter au système de l'entreprise. Il a créé un mot de passe (Martin123456) et l'a immédiatement noté pour ne pas l'oublier. Il l'a écrit sur un post-it qu'il a collé sur son poste de travail. Les instructions indiquent ensuite qu'il faut créer un profil RH en ligne. Martin a réutilisé le même mot de passe pour ne pas l'oublier. Pendant qu'il créait son profil, Martin a vu qu'il y avait un nouveau courriel dont l'objet était FÉLICITATIONS. Il n'a pas reconnu la personne qui l'avait envoyé, mais c'était normal, car il était nouveau et ne connaissait personne. Il a supposé qu'il s'agissait d'un message de bienvenue et a cliqué sur un lien inclus dans le message, ce qui a fait virer son écran au rouge et a verrouillé l'ordinateur. Martin a éteint son ordinateur, n'a rien dit à personne et est allé voir s'il pouvait obtenir son équipement de protection individuelle (ÉPI).

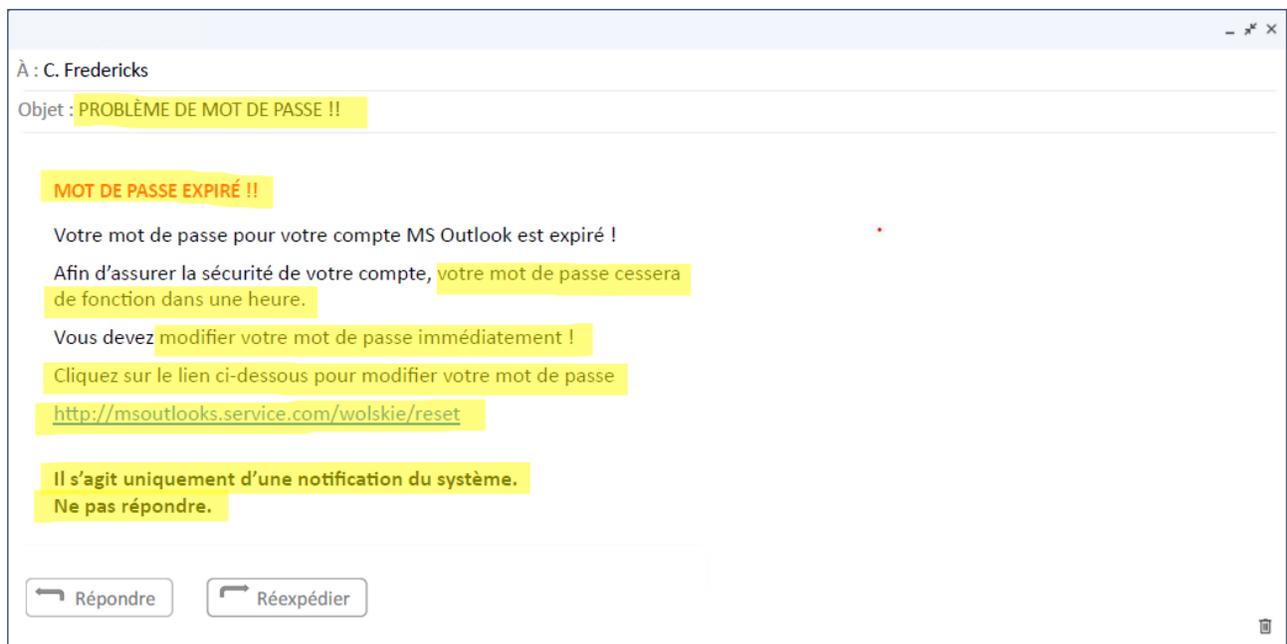
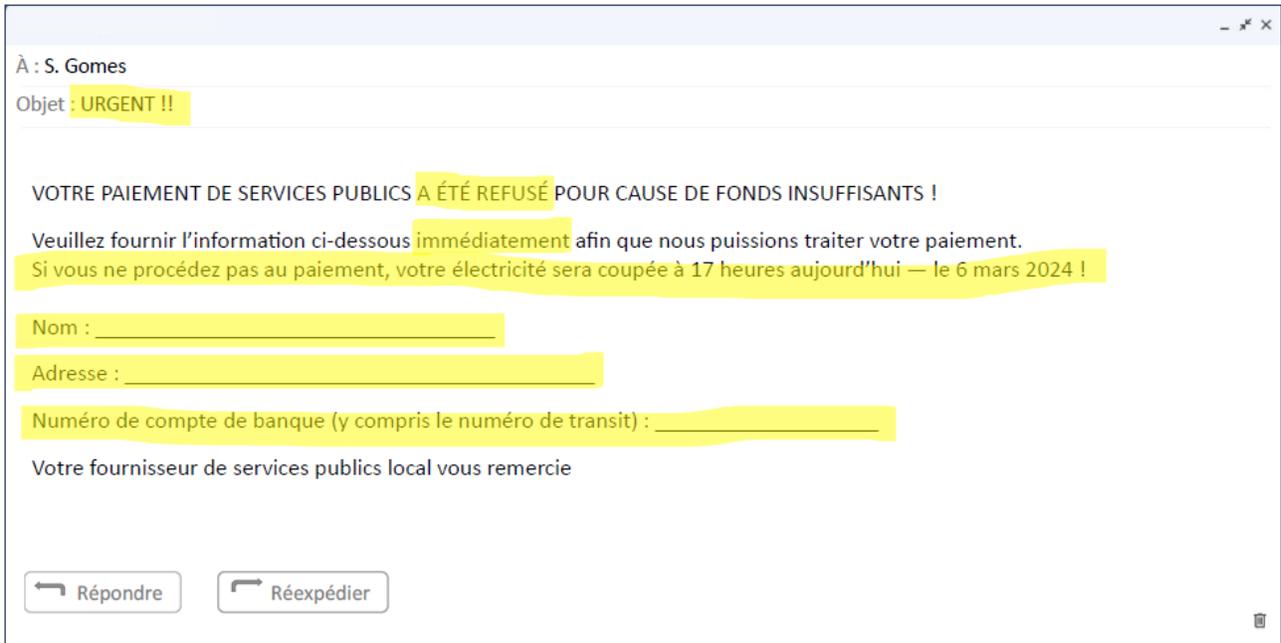


1.

Dans chacun des courriels de la page suivante, surlignez trois indices indiquant qu'il pourrait s'agir d'une attaque par hameçonnage.

(Compétences numériques, niveau intermédiaire)

Voici les trois réponses possibles.







### 3. GÉRER LES MÉDIAS SOCIAUX AVEC INTELLIGENCE

1. Utilisez les informations tirées des deux situations pour compléter le tableau.  
(Compétences digitales, niveau intermédiaire)  
Les réponses devraient ressembler à celle-ci.

	Joueur de football	Entrepreneur chez Chrysler
Quelle plateforme de médias sociaux ont-ils utilisée ?	<i>Twitter (X)</i>	<i>Twitter (X)</i>
Quel type de média ont-ils publié (vidéo, commentaire, etc.) ?	<i>Gazouillis</i>	<i>Gazouillis</i>
Pourquoi la publication était-elle inacceptable ?	<i>A tenu des propos homophobes.</i>	<i>A utilisé un langage obscène.</i>
Qu'est-il arrivé à la personne qui a affiché le message ?	<i>Sa réputation a été ternie.</i>	<i>A perdu son emploi</i>
Qu'aurait pu faire chaque personne qui a émis un gazouillis pour éviter le problème ?	<i>Il aurait dû faire le ménage dans ses médias sociaux avant d'entrer au collège.</i>	<i>Il aurait dû vérifier qu'il publiait sur le bon compte et qu'il n'avait pas utilisé d'obscénité.</i>
Pensez-vous que la réaction au gazouillis du joueur de football était juste ? Pourquoi ou pourquoi pas ? <i>Les réponses peuvent varier</i>		
Pensez-vous que la réaction au gazouillis de l'entrepreneur était juste ? Pourquoi ou pourquoi pas ? <i>Les réponses peuvent varier</i>		



Passez en revue la liste des plateformes en ligne populaires ci-dessous et mettez un ✓ à côté de chacune de celles que vous utilisez. Ajoutez les autres qui ne figurent pas dans la liste dans les lignes vides. Remplissez ensuite les colonnes restantes pour celles que vous avez sélectionnées.

*(Compétences numériques, niveau de base) Les réponses peuvent varier. Quelques exemples ci-joints.*

Plateforme	✓ si vous l'utilisez	Nombre de fois par semaine que vous affichez quelque chose	Nombre de fois par semaine que vous affichez un commentaire ou partagez l'information de quelqu'un d'autre
Facebook	✓	3	2
Instagram	✓	6	5
Twitter/X	✓	5	8
YouTube			
LinkedIn	✓	1	3
Snapchat			
TikTok			
Total de publications, de commentaires et de messages partagés par semaine		15	18
Total des publications, de commentaires et de messages partagés par année		780	936
Nombre total de pièces d'information partagées entre la 8 <sup>e</sup> année et l'obtention de son diplôme		3 900	4,680



1.

Deux des choses les plus importantes que vous puissiez faire pour protéger votre identité sont de comprendre comment fonctionne la protection de la confidentialité en ligne et de vérifier régulièrement vos paramètres.

Indiquez si chaque affirmation ci-dessous est vraie ou fausse. Si l'affirmation est fausse, réécrivez-la pour qu'elle soit vraie (la première est déjà faite pour vous).

*(Compétences numériques, niveau intermédiaire)*

*Les réponses peuvent varier. Quelques exemples présentés.*

<p>Les paramètres de confidentialité assurent une protection totale. <b>VRAI FAUX</b>  <i>Les paramètres de confidentialité n'offrent pas une protection totale</i></p>
<p>Partager des informations personnelles en ligne, comme votre adresse, est sans danger. <b>VRAI FAUX</b>  <i>Il n'est pas prudent de communiquer en ligne des informations personnelles telles que votre adresse.</i></p>
<p>Les paramètres de confidentialité peuvent être modifiés. <b>VRAI FAUX</b></p>
<p>Les paramètres de confidentialité sont un bon moyen de protéger la confidentialité des informations. <b>VRAI FAUX</b></p>
<p>Public signifie que tout le monde sur le site d'un média social peut voir ce que vous publiez. <b>VRAI FAUX</b></p>
<p>Se connecter à une application à partir d'une autre est rapide et sûr. <b>VRAI FAUX</b>  <i>C'est peut-être rapide, mais il n'est pas sûr de se connecter à une application à partir d'une autre.</i></p>
<p>Une fois que vous avez lu une politique de confidentialité, vous n'avez plus besoin de lire les mises à jour. <b>VRAI FAUX</b>  <i>Vous devez lire les mises à jour de la politique de confidentialité.</i></p>



Les paramètres de confidentialité coutent plus cher. VRAI FAUX

*Les paramètres de confidentialité ne coutent pas plus cher.*

1.

Que signifie exactement cette politique ? Pour vous assurer que vous comprenez ce qu'ils disent, associez les synonymes aux mots de l'article.

(Compétences numériques, niveau intermédiaire)

FROM THE ARTICLE	SYNONYMS
Facteur d'incertitude	<i>Quelque chose de difficile à prédire</i>
Établissement postsecondaire	<i>Collèges et universités</i>
Au cas par cas	<i>Individuellement</i>
Évaluer	<i>Juger</i>
Critères	<i>Standards</i>

2.

Complétez chaque phrase par « fait » ou « ne fait pas » pour la rendre vraie.

(Compétences numériques, niveau intermédiaire)

L'université *ne fait pas* la vérification des médias sociaux de ses candidats.

L'université *fait* la vérification des médias sociaux des étudiants inscrits.

L'université *fait* en sorte que les étudiants sont responsables de ce qu'ils affichent en ligne.

L'université *ne fait pas* en sorte que l'on traite chaque cas de la même façon.



## 4. QUESTION D'ARGENT EN LIGNE

1.

Remplissez les tirets pour que les phrases aient un sens.  
(Compétences numériques, niveau intermédiaire)

Lors d'une fraude, un pirate informatique vole vos informations, généralement financières.

Lors d'une arnaque, on vous incite à fournir des informations personnelles.

1.

À l'aide des informations que vous venez de lire, placez un X dans les colonnes correspondant à chaque technique et au type d'arnaque dans lequel elle est le plus souvent utilisée. Attention, des arnaques différentes peuvent utiliser les mêmes techniques.  
(Compétences numériques, niveau intermédiaire)

TECHNIQUE	RELATIONS AMOUREUSES	EMPLOI	MAGASINAGE
Gagner votre confiance	X	X	
Offrir quelque chose de trop beau pour être vrai		X	
Envoyer un faux transfert d'argent			X
Demander des informations d'identification personnelle		X	



Indiquer que c'est urgent	X	X	
Ne pas envoyer ce qui a été promis			X
Vous donner l'impression d'être important		X	
Demander un type de paiement inhabituel			X
Effectuer le premier contact via les médias sociaux	X		

2.

À l'aide des informations fournies dans la boîte de texte, quelles images ou quels mots affichés sur un site Web vous indiquent que vous pouvez y magasiner avec votre carte de crédit en toute sécurité ? Cochez toutes les cases correspondantes.

(Compétences numériques, niveau intermédiaire)

Magasiner sur un site Web sécurisé

1. Un crochet vert
2. Le mot sécurisé
3. Le mot buysafe
4. Un symbole de serrure
5. Un crochet rouge
6. Le mot http
7. Le mot ccsafe
8. Le mot https
9. Le mot safe
10. Le mot SSL

N'achetez jamais rien en ligne avec votre carte de crédit sur un site qui n'est pas équipé du système de cryptage SSL (*secure sockets layer*—couches d'échange sécurisées). Vous saurez que le site utilise le protocole SSL parce que l'URL du site commencera par HTTPS — au lieu de HTTP. Une icône représentant un cadenas verrouillé apparaît également, généralement à gauche de l'URL dans la barre d'adresse ou dans la barre au-dessous ; cela dépend de votre navigateur. Le protocole HTTPS est maintenant la norme, même sur les sites qui ne sont pas destinés au magasinage, au point que Google Chrome signale toute page dépourvue du S comme « non sécurisée ».



1.

Faites la lecture de chaque scénario et identifiez dans chacun d'eux au moins 3 indices qui auraient dû aider la victime à reconnaître qu'on tentait de l'arnaquer. Inscrivez vos réponses dans les espaces fournis.

*(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier. Des exemples de réponses sont présentés.*

### Scénario 1

À la dernière minute, Karrie a voulu acheter deux billets pour un festival de musique d'été. Toutefois, le site Web officiel indiquait qu'il n'y avait plus de places disponibles. Elle a trouvé quelqu'un en ligne qui avait deux billets disponibles pour 150 \$ chacun. Elle a pensé que c'était une très bonne affaire et a accepté d'envoyer 300 dollars en utilisant PayPal. Le vendeur a déclaré qu'il préférerait les cartes-cadeaux parce qu'il avait déjà été victime d'une arnaque et qu'il savait maintenant que les cartes-cadeaux étaient « plus sûres » que PayPal. Il a également dit qu'il était vraiment désolé de ne pas pouvoir aller au festival, mais qu'il avait un besoin urgent de vendre les billets. Il a ajouté qu'il ne pouvait pas les garder en attendant qu'elle prenne une décision. Karrie a trouvé cela étrange, mais le type avait l'air sympa. Elle a donc accepté et a acheté trois cartes-cadeaux de 100 \$ en ligne et lui a envoyé les informations. Une fois les cartes échangées, il l'a immédiatement bloquée sur Facebook. Finalement, elle n'avait pas de billets, pas de remboursement, et aucun moyen de retrouver l'homme en question.

Identifiez au moins 3 indices

*Le vendeur a dit qu'il avait besoin de vendre tout de suite –  
impression d'urgence*

---

*On lui a demandé d'effectuer un paiement d'une manière spécifique*

---

*Revendeur non officiel*

---

### Scénario 2

Devrin venait de commencer son premier véritable emploi après l'école et voulait offrir un cadeau à ses parents pour les remercier de leur aide au fil des ans. Sachant que le barbecue familial commençait à se faire vieux, Devrin a cherché une bonne affaire en ligne. Il a trouvé un site Web qui proposait des barbecues de marque à des prix ridiculement réduits. Le site indiquait qu'il s'agissait d'une nouvelle entreprise, que les bas prix faisaient partie de leurs promotions de lancement et qu'il s'agissait d'une « offre à durée limitée ». La seule condition était de faire une demande de crédit et de payer avec la carte de crédit de



l'entreprise. Le taux de la carte était très compétitif, à seulement 2,9 %. Devrin a effectué une recherche en ligne sur l'entreprise et n'a pas trouvé de mauvaises critiques. Il a donc demandé la carte sur le site Web de l'entreprise et l'a utilisée pour payer le barbecue. Une semaine plus tard, il a reçu un courriel l'informant qu'en raison de problèmes liés à la chaîne d'approvisionnement, la livraison du barbecue avait été retardée. On lui a aussi indiqué que, puisque l'entreprise n'était pas responsable de ce retard, il ne pouvait pas obtenir un remboursement. Devrin est immédiatement retourné voir le site Web de l'entreprise, mais celui-ci avait disparu. Le barbecue n'a jamais été livré et il n'a jamais été remboursé.

Identifiez au moins 3 indices

*Le prix est trop beau pour être vrai*

---

*Offre à durée limitée – impression d'urgence*

---

*On lui a demandé d'effectuer un paiement d'une manière précise*

---

### Scénario 3

Alix a rencontré son partenaire Seamus sur Facebook. Ils ont échangé des textos et clavardé en ligne pendant plusieurs mois, et leur relation est devenue plus sérieuse au fil du temps. Seamus a déclaré qu'il vivait en Irlande, mais qu'il était prêt à déménager au Canada pour voir où leur relation pourrait aller. Il a envoyé à Alix les informations concernant son vol et lui a dit qu'il avait déjà expédié ses affaires. Le jour du vol, Alix a reçu un appel d'un agent des douanes lui annonçant que la cargaison était arrivée, mais qu'il fallait payer les douanes. On lui a dit qu'on avait essayé de joindre Seamus, mais qu'on n'avait pas pu le faire, car il était en transit. Le numéro d'Alix se trouvait sur la cargaison en tant que personne à contacter au Canada, ils ont donc décidé de la joindre. Les douanes ont expliqué que si les douanes n'étaient pas payées immédiatement, la cargaison serait renvoyée en Irlande aux frais de Seamus. Alix a voulu aider et a donc payé le solde dû par virement bancaire, conformément aux instructions, pour un montant de 3 355,99 dollars. Elle avait déjà prêté de petites sommes d'argent à Seamus, qui les avait toujours remboursées. Elle ne s'inquiétait donc pas.

Quand Alix est arrivée à l'aéroport ce soir-là pour rencontrer Seamus, il ne s'est pas présenté. Lorsqu'elle a essayé de lui envoyer un message, il n'a pas répondu. Son profil Facebook est aussi disparu. Quelques jours plus tard, Alix s'est rendu compte qu'elle avait été victime d'une arnaque. Elle a demandé à sa banque de récupérer le paiement, mais l'argent avait déjà été transféré et elle n'a pas obtenu gain de cause.



Identifiez au moins 3 indices

*Appel des douanes – contact inattendu (en fait, les douanes n'appellent jamais)*

---

*Paiement immédiat exigé – impression d'urgence*

---

*Demandes d'argent antérieures*

---

*Il a gagné sa confiance*

---



1.

Cochez toutes les affirmations pertinentes.  
(Compétences numériques, niveau intermédiaire)

LES FRAUDES SONT POSSIBLES, CAR :	✓
Les gens sont stupides	
Les gens veulent faire de bonnes affaires	✓
Les gens utilisent des téléphones portables	
Les arnaqueurs sont intelligents	✓
Les gens aiment se sentir spéciaux	✓
Les gens ne reçoivent pas assez de courriels	
Les arnaqueurs savent comment manipuler les gens	✓

2.

Indiquez si les affirmations ci-dessous sont vraies ou fausses.  
(Compétences numériques, niveau intermédiaire)

AFFIRMATIONS	VRAI	FAUX
La durée d'attention typique est de 8 minutes.		✓
La peur de manquer sa chance est une cause réelle d'arnaque.	✓	
Toute personne âgée utilisant Internet peut être victime d'une arnaque.	✓	
La manipulation psychologique ne fonctionne pas.		✓
Certaines personnes se font piéger parce qu'elles sont seules.	✓	
Seuls 7 % des courriels frauduleux sont urgents.		✓
Certaines personnes se font arnaquer parce qu'elles se croient plus intelligentes que les autres.	✓	



1.

Faites correspondre le type de paiement utilisé avec l'endroit où vous devez le signaler si vous êtes victime d'une fraude.

*(Compétences numériques, niveau intermédiaire)*

Type de paiement	Signalez la fraude à...
Application de transfert de fonds	<i>L'entreprise propriétaire de l'application</i>
Carte de crédit	<i>Votre banque</i>
Virement bancaire	<i>Votre banque</i>
Carte-cadeau	<i>L'entreprise qui émet la carte-cadeau</i>
Cryptomonnaie	<i>La bourse d'échange</i>





## 5. UTILISER L'IA

1.

Les informations ci-dessous sont basées sur un graphique de 2021 publié par Statista. (<https://www.statista.com/chart/29229/areas-of-life-most-expected-to-change-by-the-use-of-ai/>)

Le graphique décrit les domaines de la vie qui, selon les personnes interrogées, changeront le plus à cause de l'utilisation accrue de l'IA entre 2021 et 2026. L'échantillon de population participant à l'étude était composé de 19 504 personnes âgées de 16 à 74 ans originaires de 28 pays. Utilisez les informations pour répondre aux questions.

*(Compétences numériques, niveau intermédiaire)*

Pourcentage des personnes interrogées qui s'attendent à ce que les domaines suivants subissent les changements les plus importants en raison de l'utilisation de l'IA au cours des 3 à 5 prochaines années.

35 % — Éducation	32 % — Emploi
30 % — Transport	26 % — Cout de la vie
23 % — Salaires	15 % — Nourriture et nutrition
33 % — Sécurité	31 % — Magasinage
27 % — Divertissement	23 % — Foyer
22 % — Environnement	15 % — Relations personnelles

Quel est le domaine pour lequel la plupart des gens pensent qu'il y aura le plus grand changement ?

*Éducation*

Quel est le domaine dans lequel vous pensez que les changements seront les plus importants ? Justifiez votre réponse.

*Les réponses peuvent varier.*

Quel est le domaine pour lequel la plupart des gens pensent qu'il y aura le moins de changements ?



*Nourriture et nutrition et relations personnelles*

Quel est le domaine pour lequel vous pensez qu'il y aura le moins de changements ? Justifiez votre réponse.

*Les réponses peuvent varier.*

2.

Il est important de connaître le sens de ces différents mots dans le contexte de l'IA. Dans le tableau suivant, associez à chaque mot la définition qui vous semble la plus appropriée, en traçant une ligne entre les deux.

*(Compétences numériques, niveau intermédiaire)*

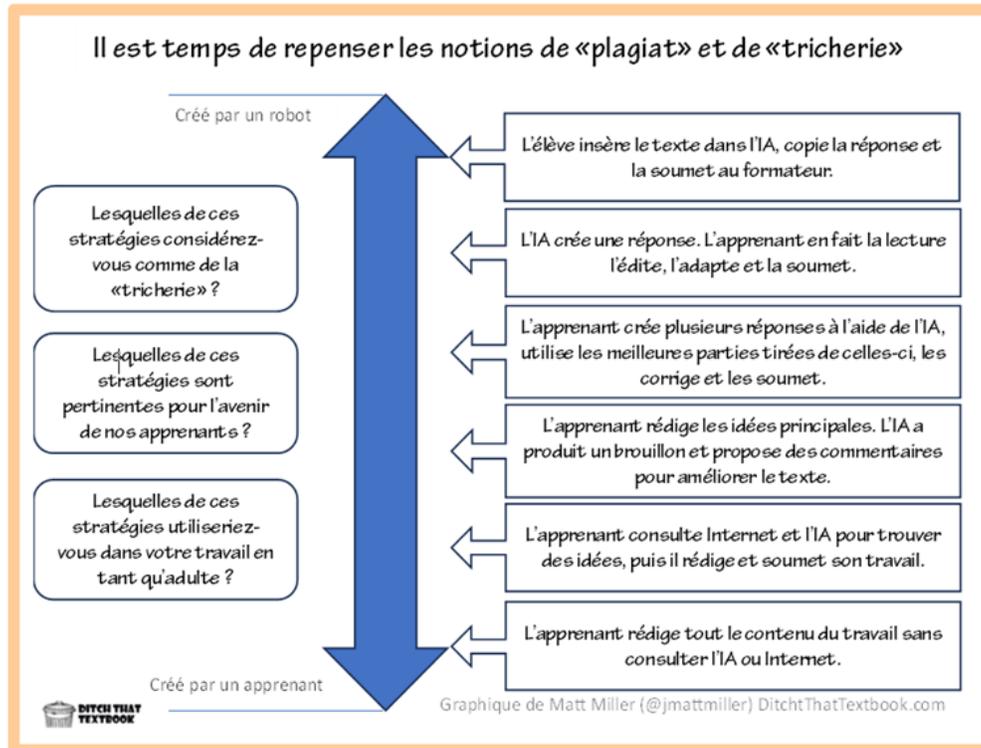
MOTS	DÉFINITIONS
Plagiat	Faits faux ou inexacts.
Éthique	Prédictions ou résultats qui favorisent ou discriminent des groupes spécifiques de personnes.
Désinformation	Lorsqu'une personne présente un certain type de travail comme étant sa propre création alors qu'en réalité il ne s'agit pas de son travail.
Biais	Lorsqu'une personne fait quelque chose de malhonnête dans le cadre d'un travail académique ou professionnel qui donne une fausse représentation de ce qu'elle comprend ou de ce qu'elle peut faire, lui procurant ainsi un avantage injuste.
Trichage	Ensemble de principes moraux suivis par des personnes généralement considérées comme bonnes.



3.

Consultez le graphique de la page suivante, créé pour les enseignants, qui montre comment les élèves utilisent l'IA comme ChatGPT. Parmi les actions de droite, lesquelles vous semblent être de la tricherie ?

(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier. Quelques modèles de réponses fournis.



<https://ditchthattextbook.com/ai/> (traduit)

*Exemple de réponse*

Seule la première action de la liste, pour laquelle l'apprenant a pris ce que l'IA lui présentait, l'a copié mot pour mot et l'a remis comme son propre travail, serait peut-être considérée comme de la tricherie. Pour toutes les autres actions, l'apprenant a interagi avec le texte pour le comprendre et le réviser ou a choisi de ne pas utiliser l'IA.



4.

Rédigez trois règles simples qui, selon vous, seraient utiles pour aider les apprenants à comprendre quand ils peuvent utiliser le ChatGPT et pour s'assurer que son utilisation se fait dans le respect de l'éthique.

*(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier. Un exemple de réponses est fourni.*

1. Utilisez-le pour améliorer votre travail, pas pour le créer.
2. Utilisez-le pour vérifier la grammaire et l'orthographe.
3. Utilisez-le pour fournir de bons exemples.
4. Si vous pensez que vous l'avez trop utilisé, vous avez probablement raison.
5. Ne croyez pas que tout ce qui est écrit est vrai.
6. Assurez-vous de pouvoir répondre à des questions sur ce que ChatGPT a écrit pour vous.

5.

Examinez cette utilisation réelle en lien avec l'IA, rapportée dans le Toronto Life Magazine, et répondez aux questions qui suivent.

*(Compétences numériques, niveau intermédiaire)*

Quel autre outil numérique l'étudiant a-t-il utilisé en plus de ChatGPT

*Des bases de données*

---

Qu'est-ce que l'étudiant a écrit dans ChatGPT ?

*Une description de l'échantillon du sol*

---

Quelle erreur ChatGPT a-t-il corrigée ?

*La couche de goudron datait des années 1950 et non des années 1970.*

---

Croyez-vous que l'étudiant ait triché ou qu'il a utilisé ChatGPT de manière éthique ? Justifiez votre réponse. *(Les réponses peuvent varier)*



**1.** Répondez aux 3 questions ci-dessous.  
(*Compétences numériques, niveau intermédiaire*)

Quelle est la différence la plus importante entre l'automatisation et l'IA ?

*L'automatisation ne peut que répéter les tâches pour lesquelles une machine est programmée. Toutefois, l'IA peut être programmée pour détecter quand les choses tournent mal, trouver comment les réparer, apprendre de ces expériences et améliorer leur fonction.*

À l'aide des informations contenues dans l'article, décrivez un avantage de l'utilisation de l'IA dans chacun des secteurs énumérés.

- Fabrication : *augmenter la sécurité ou réduire les coûts*
- Construction : *améliorer l'efficacité ou réduire les coûts*
- Agriculture : *aider les agriculteurs à mieux planifier ou à améliorer le rendement des cultures*

Que pourra faire le nouveau robot d'entrepôt que les robots actuels ne peuvent pas faire ?  
*Se déplacer dans l'usine.*





## 6. LA SANTÉ NUMÉRIQUE

1.

Lisez l'article intitulé « Limiter les risques de l'autodiagnostic ». Il porte sur les inconvénients possibles de l'utilisation d'Internet pour obtenir des informations sur la santé. Par la suite, utilisez les mots figurant dans les bulles pour compléter les affirmations.  
(Compétences numériques, niveau intermédiaire)

1. Cherchez des sites Web que *modèrent* des agences de la santé ou gouvernementales.
2. Un mauvais diagnostic peut *retarder* l'obtention du bon traitement.
3. Plusieurs maladies graves peuvent avoir des symptômes *banals*.

La *désinformation* est un problème commun lorsque l'on trouve des informations en lien avec votre santé sur les médias sociaux.

4. N'utilisez les sites Web que pour *diagnostiquer* les maladies bénignes.

2.

Pour chacun des risques énumérés dans le tableau, identifiez au moins une action que vous pouvez entreprendre pour réduire le risque.  
(Compétences numériques, niveau intermédiaire) Les réponses devraient être semblables à celles retrouvées ici.

RISK	ACTION
Suivre des instructions inexactes	Vérifiez les auteurs ou propriétaires des sites Web. Recherchez des organismes fiables.



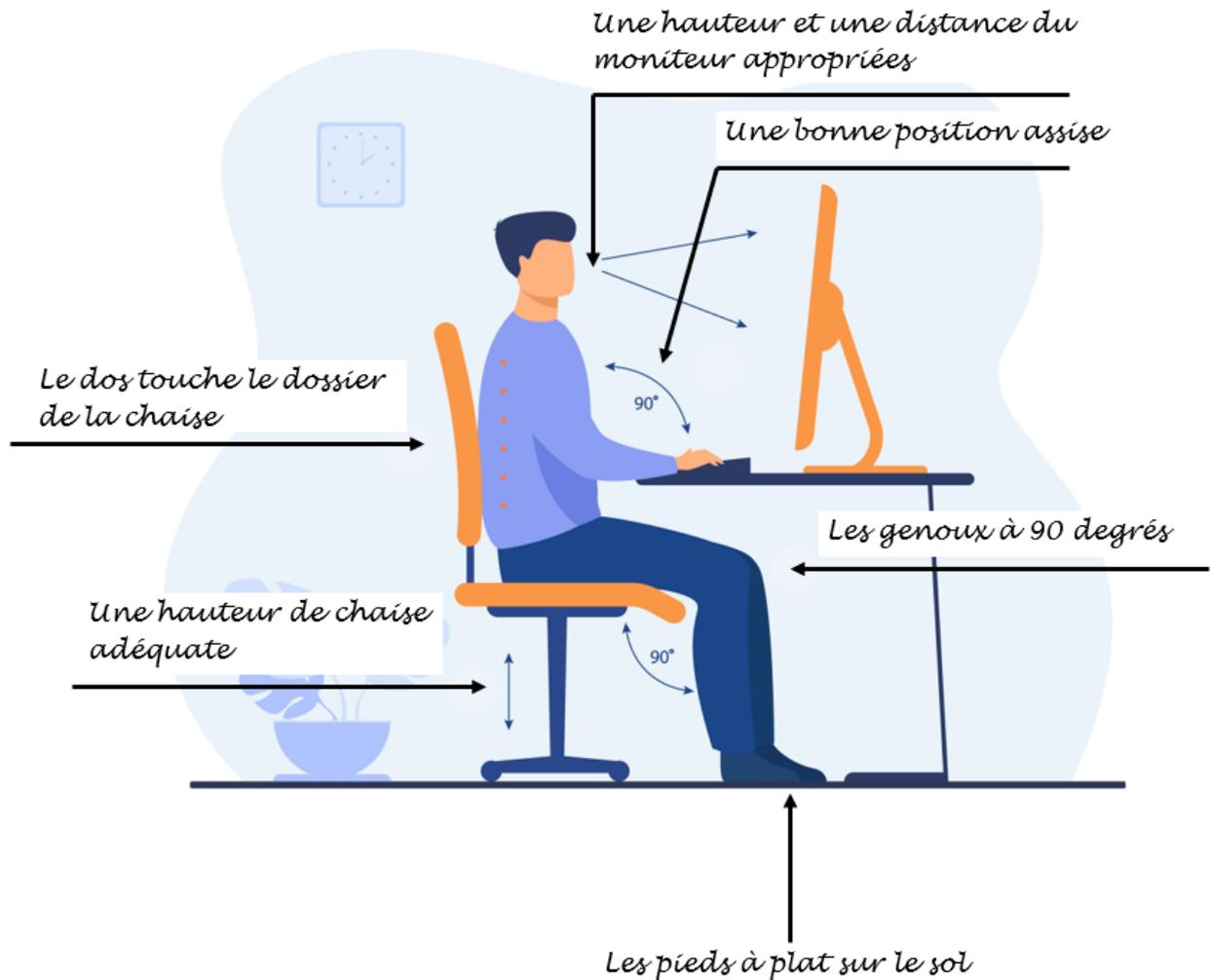
Perte d'informations personnelles	<p><i>Ne fournissez pas d'informations sur les sites Web consacrés à la santé.</i></p> <p><i>Ne vous abonnez pas.</i></p>
Augmenter votre niveau d'anxiété	<p><i>Limitez le nombre de sites Web que vous consultez.</i></p> <p><i>Ne consultez que des sites fiables.</i></p> <p><i>Consultez un professionnel de la santé.</i></p>
Retarder l'obtention des soins médicaux dont vous avez besoin	<p><i>Utilisez les recherches sur Internet que pour des maladies bénignes.</i></p> <p><i>Consultez un professionnel de la santé.</i></p>
Perdre du temps et de l'argent avec de faux remèdes	<p><i>Ne consultez que des sites fiables.</i></p>



1.

Utilisez les informations de l'article « Parlons des aspects physiques » pour identifier les précautions ergonomiques prises par la personne pour prévenir les problèmes musculosquelettiques et de fatigue des yeux sur l'image.

(Compétences numériques, niveau intermédiaire)



2.

Utilisez les informations dans le diagramme des niveaux de bruit pour répondre aux questions.

(Compétences numériques, niveau intermédiaire)

1. Quelle est la différence en décibels entre entendre du matériel d'aménagement paysager à l'extérieur ou à l'intérieur d'une maison ? 35
2. Prendre l'avion peut-il nuire à votre audition ? Encerclez votre réponse.  OUI  NON



3. Quel est le seuil de sécurité des sons ? 70
4. À combien de dB du niveau de sécurité se situe un sèche-cheveux ? 20
5. À part l'avion, quel est le bruit de transport le plus fort ? *Sirène*
6. Quelle est la différence en décibels entre un sèche-mains électrique et un sèche-cheveux ? 10

## 3.

En plus de mieux gérer vos appareils numériques, il y a d'autres choses que vous pouvez faire pour améliorer la qualité de votre sommeil. Utilisez les informations que vous venez de lire et l'infographie de Santé publique Canada, à la page suivante, pour répondre aux questions.  
(*Compétences numériques, niveau intermédiaire*)

1. Quel pourcentage d'adultes de moins de 35 ans ne dort pas assez ? 25 %
2. Quel pourcentage des adultes a du mal à rester endormi ? 50 %
3. Quel pourcentage des adultes pourrait s'endormir au cours de la journée ? 33 %
4. Compte tenu de votre âge, combien d'heures devriez-vous dormir chaque nuit ?  
*7 à 9 heures*
5. Combien d'heures dormez-vous ? \_\_\_\_\_ *Les réponses peuvent varier.*
6. Si vous dormez moins que le nombre d'heures recommandées, identifiez deux changements que vous pourriez apporter à vos habitudes de sommeil. *Les réponses peuvent varier.*

## 4.

Remplissez l'autoévaluation suivante de Santé Canada pour évaluer votre niveau d'activité physique.  
(*Compétences numériques, niveau intermédiaire*)  
*Les réponses peuvent varier.*



5.

Définissez dans vos propres mots les termes suivants trouvés dans cette séance de formation.

(Compétences numériques, niveau intermédiaire)

Ergonomie :

*L'étude des personnes dans leur environnement de travail*

Interaction :

*Lorsque deux ou plusieurs éléments fonctionnent ensemble*

Cyberchondrie :

*Un type de trouble de l'anxiété lié à la recherche de maladies sur Internet*

Musculosquelettique :

*Se rapportant aux muscles et aux os*

Décibel:

*Une unité de mesure du son*

Précautions:

*Les mesures prises pour prévenir les problèmes ou les blessures*

Corrélation:

*Lorsqu'une chose a un impact direct sur une autre*

IPE :

*Équipement de protection individuelle*



1.

Soulignez la meilleure solution d'un impact négatif d'une utilisation excessive de la technologie pour chaque exemple.

(Compétences numériques, niveau intermédiaire)

Ne pas pouvoir dormir	A. Faire une promenade matinale.
	B. <u>Se déconnecter de toute technologie 30 minutes avant de se coucher.</u>
Subir de la cyberintimidation	A. <u>En parler à un adulte responsable.</u>
	B. Les ignorer, ils finiront par s'arrêter.
Avoir des douleurs constantes au cou	A. <u>Essayer de tenir son téléphone plus haut que ses genoux.</u>
	B. Arrêter d'utiliser des écouteurs.
Vérifier constamment votre téléphone	A. Programmer de l'activité physique à votre horaire.
	B. <u>Programmer des heures fixes pour consulter ses messages.</u>
Se sentir isolé et déprimé	A. <u>Parler à un ami ou à un conseiller en personne.</u>
	B. Dire à un nouvel ami en ligne ce que vous ressentez.

2.

Faites la lecture de l'histoire de Juno, puis complétez le tableau pour identifier trois effets négatifs qu'elle subit et une solution possible pour chacun d'entre eux.

(Compétences numériques, niveau intermédiaire) Les réponses peuvent varier. Un exemple de réponse est fourni.

IMPACT NÉGATIF	SOLUTION POTENTIELLE
Elle éprouve des sentiments d'anxiété, de solitude et la pression constante d'être toujours « dans le coup »	<p>Passer plus de temps avec des personnes dans la vie réelle.</p> <p>Prendre des pauses de son téléphone.</p> <p>Parler à un professionnel de la santé mentale.</p>



<p><i>Elle dort rarement bien</i></p>	<p><i>Retirer le téléphone de sous son oreiller.</i></p> <p><i>Laisser le téléphone à l'extérieur de sa chambre à coucher.</i></p> <p><i>Faire une activité sans écran avant de se coucher.</i></p>
<p><i>Elle souffre constamment de douleurs au cou et au dos; elle a mal aux yeux</i></p>	<p><i>Revoir les conseils ergonomiques concernant la posture et la réduction de la fatigue visuelle.</i></p> <p><i>Faire des mini-pauses pour éviter d'être assise et devant un écran aussi longtemps.</i></p>



**PROGRAMME COMPÉTENCE  
POUR RÉUSSIR POUR LES  
JEUNES PRÊTS À TRAVAILLER**



**ÉVALUATION DES  
COMPÉTENCES  
POUR RÉUSSIR**

# COMPÉTENCES NUMÉRIQUES

Utilise la table des matières pour naviguer dans ce cahier d'activités. Suis ta progression en cochant chaque sujet terminé.

PARTIE ET SUJET		Page	√
QUESTIONS POUR TESTER TES COMPÉTENCES!		171	
1	Compétences Numériques : Questions pour tester tes compétences	173	
2	Compétences Numériques : Questions pour tester tes compétences - Réponses	179	



## 1. COMPÉTENCES NUMÉRIQUES QUESTIONS ÉVALUANT LES COMPÉTENCES

**ESSAYEZ DE RÉPONDRE AUX 14 QUESTIONS CI-DESSOUS,  
PUIS CONSULTEZ LE CORRIGÉ POUR VOIR OÙ VOUS EN ÊTES.**

Selon cette description, quelle affirmation est correcte ?

**1.**

Le Japon et la Commission européenne ont identifié une possible 5<sup>e</sup> révolution axée non seulement sur la technologie numérique, mais aussi sur la manière dont cette technologie peut être utilisée pour améliorer la société. Pour les travailleurs, l'Industrie 5.0 consiste à laisser l'automatisation et les robots accomplir des tâches répétitives tout en leur permettant de se consacrer à d'autres activités.

Au cours de l'Industrie 5.0 :

- a) Les robots remplaceront tous les travailleurs.
- b) Les robots rendront les emplois des travailleurs plus intéressants.
- c) Les travailleurs remplaceront certains robots.

**2.**

Faites correspondre les tâches aux outils numériques les plus utilisés en inscrivant le numéro de la tâche à côté de l'outil approprié.

OUTIL NUMÉRIQUE	N° DE TÂCHE
Bases de données	
Logiciels de communication	
Traitement de texte	
Logiciel de feuille de calcul	
Internet	

### TÂCHES

1. Remplir un rapport de sécurité.
2. Comparer les coûts des matériaux de fournisseurs différents.
3. Calculer l'impact d'une augmentation de 15 % des matériaux.
4. Informer votre superviseur de votre retard.
5. Vérifier la disponibilité d'un produit.



**3.**

Dans le contexte des outils et processus numériques, l'AMF signifie :

- a) Accès à plusieurs facteurs
- b) Authentification multifactorielle
- c) Admission multifactorielle

**4.**

Quels sont les trois facteurs les plus souvent utilisés pour l'AMF ?

- a) Qui vous êtes, ce que vous voulez, ce que vous savez
- b) Ce que vous savez, ce que vous avez, où vous êtes
- c) Ce que vous avez, ce que vous savez, ce que vous êtes

**5.**

Indiquez si chaque affirmation est vraie ou fausse.

- a) Les paramètres de confidentialité assurent une protection totale. V F
- b) Le partage des mots de passe lorsque l'on travaille sur le même projet est sécuritaire. V F
- c) Les courriels portant la mention « important » sont toujours sûrs. V F

De quel type d'arnaque s'agit-il ?

**6.**

Marc reçoit un message sur FB en réponse à un article qu'il a partagé sur une nouvelle entreprise technologique lancée à Montréal. L'expéditeur dit travailler pour l'entreprise et remercie Marc d'avoir partagé le message. Il invite ensuite Marc à cliquer sur un lien pour s'inscrire à la première série d'entrevues, ce qui signifie que Marc obtiendra une entrevue avant tout le monde.

- a) Arnaque liée au magasinage
- b) Arnaque liée à l'emploi
- c) Arnaque liée aux relations amoureuses



7.

Si vous pensez avoir été victime d'un hameçonnage au travail, quelle est la première chose à faire ?

- a) Éteignez votre ordinateur.
- b) Supprimez le courriel.
- c) Informez votre supérieur.

8.

Placez un crochet (✓) pour tous les appareils qui utilisent l'AI.

Perceuse électrique	
Soudeur au laser	
Gilet de sécurité	
GPS	
Téléphone intelligent	
Station de lavage des yeux	



9.

Il est important de connaître le sens de ces différents mots dans le contexte de l'IA. Dans le tableau suivant, associez à chaque mot la définition qui vous semble la plus appropriée, en traçant une ligne entre les deux.

MOTS	DÉFINITIONS
Plagiat	Faits faux ou inexacts.
Éthique	Prédictions ou résultats qui favorisent ou discriminent des groupes spécifiques de personnes.
Désinformation	Lorsqu'une personne présente un certain type de travail comme étant sa propre création alors qu'en réalité il ne s'agit pas de son travail.
Biais	Lorsqu'une personne fait quelque chose de malhonnête dans le cadre d'un travail académique ou professionnel qui donne une fausse représentation de ce qu'elle comprend ou de ce qu'elle peut faire, lui procurant ainsi un avantage injuste.
Trichage	Ensemble de principes moraux suivis par des personnes généralement considérées comme bonnes.

10.

Pourquoi l'AMF est-elle utile ?

- Elle permet de partager les mots de passe en toute sécurité.
- Elle facilite la connexion.
- Elle ajoute une couche supplémentaire de protection numérique.

11.

L'ergonomie, c'est :

- l'étude de l'ego
- l'étude de l'environnement physique de travail des personnes
- les lois naturelles du travail physique



12.

Placez un crochet (✓) pour toutes les suggestions qui peuvent vous aider à éviter l'inconfort ou les blessures lorsque vous travaillez avec de la technologie numérique.

Assurez-vous que vos genoux forment un angle de 90 degrés quand vous êtes assis.	
Utilisez toujours vos pouces pour taper des messages sur votre téléphone.	
Tenez votre téléphone sur vos genoux lorsque vous envoyez des textos.	
Faites régulièrement de courtes pauses lorsque vous travaillez à l'écran.	
Installez votre moniteur pour que le haut soit à la hauteur des yeux.	
Maintenez l'éclairage à un niveau élevé.	

13.

La cyberchondrie, c'est :

- a) La peur des cyborgs
- b) La crainte d'une maladie grave fondée sur des recherches de symptômes sur Internet
- c) Un moyen raisonnablement fiable de déterminer si l'on a un rhume ou une grippe

14.

Associez chaque exemple d'impact négatif possible d'un excès de technologie à une stratégie efficace pour réduire cet impact.

EXEMPLE	N° DE STRATÉGIE
Vous vivez de la cyberintimidation	
Votre cou fait mal	
Vous ne pouvez pas dormir	
Vous vous sentez isolé	

1. Arrêter le temps d'écran 30 minutes avant le coucher.
2. Planifiez une activité avec un ami de confiance en personne.
3. Surveillez la façon dont vous tenez votre téléphone.
4. Parlez-en à un adulte en qui vous avez confiance.





## 2. COMPÉTENCES NUMÉRIQUES

### QUESTIONS ÉVALUANT LES COMPÉTENCES

### RÉPONSES

#### COMMENT AVEZ-VOUS RÉPONDU AUX 14 QUESTIONS ?

Selon cette description, quelle affirmation est correcte ?

1.

Le Japon et la Commission européenne ont identifié une possible 5<sup>e</sup> révolution axée non seulement sur la technologie numérique, mais aussi sur la manière dont cette technologie peut être utilisée pour améliorer la société. Pour les travailleurs, l'Industrie 5.0 consiste à laisser l'automatisation et les robots accomplir des tâches répétitives tout en leur permettant de se consacrer à d'autres activités.

Au cours de l'Industrie 5.0 :

- b) *Les robots rendront les emplois des travailleurs plus intéressants.*

Compétences numériques — niveau intermédiaire

2.

Faites correspondre les tâches aux outils numériques les plus utilisés en inscrivant le numéro de la tâche à côté de l'outil approprié.

OUTIL NUMÉRIQUE	N° DE TÂCHE
Bases de données	2 ou 3
Logiciels de communication	4
Traitement de texte	1
Logiciel de feuille de calcul	2 ou 3
Internet	2 ou 5

#### TÂCHES

- Remplir un rapport de sécurité.
- Comparer les coûts des matériaux de fournisseurs différents.
- Calculer l'impact d'une augmentation de 15 % des matériaux.
- Informez votre superviseur de votre retard.
- Vérifier la disponibilité d'un produit.

Compétences numériques — niveau intermédiaire



**3.** Dans le contexte des outils et processus numériques, l'AMF signifie :

*b) Authentification multifactorielle*

Compétences numériques — niveau intermédiaire

**4.** Quels sont les trois facteurs les plus souvent utilisés pour l'AMF ?

*c) Ce que vous avez, ce que vous savez, ce que vous êtes*

Compétences numériques — niveau intermédiaire

**5.** Indiquez si chaque affirmation est vraie ou fausse.

- a) Les paramètres de confidentialité assurent une protection totale. V **F**
- b) Le partage des mots de passe lorsque l'on travaille sur le même projet est sécuritaire. V **F**
- c) Les courriels portant la mention « important » sont toujours sûrs. V **F**

Compétences numériques — niveau intermédiaire

De quel type d'arnaque s'agit-il ?

**6.** Marc reçoit un message sur FB en réponse à un article qu'il a partagé sur une nouvelle entreprise technologique lancée à Montréal. L'expéditeur dit travailler pour l'entreprise et remercie Marc d'avoir partagé le message. Il invite ensuite Marc à cliquer sur un lien pour s'inscrire à la première série d'entrevues, ce qui signifie que Marc obtiendra une entrevue avant tout le monde.

*b) Arnaque liée à l'emploi*

Compétences numériques — niveau intermédiaire

**7.** Si vous pensez avoir été victime d'un hameçonnage au travail, quelle est la première chose à faire ?

*c) Informez votre superviseur*

Compétences numériques — niveau intermédiaire



8.

Placez un crochet (✓) pour tous les appareils qui utilisent l'AI.

Perceuse électrique	
Soudeur au laser	✓
Gilet de sécurité	
GPS	✓
Téléphone intelligent	✓
Station de lavage des yeux	

Compétences numériques — niveau intermédiaire

9.

Il est important de connaître le sens de ces différents mots dans le contexte de l'IA. Dans le tableau suivant, associez à chaque mot la définition qui vous semble la plus appropriée, en traçant une ligne entre les deux.

Compétences numériques — niveau intermédiaire

MOTS	DÉFINITIONS
Plagiat	Faits faux ou inexacts.
Éthique	Prédictions ou résultats qui favorisent ou discriminent des groupes spécifiques de personnes.
Désinformation	Lorsqu'une personne présente un certain type de travail comme étant sa propre création alors qu'en réalité il ne s'agit pas de son travail.
Biais	Lorsqu'une personne fait quelque chose de malhonnête dans le cadre d'un travail académique ou professionnel qui donne une fausse représentation de ce qu'elle comprend ou de ce qu'elle peut faire, lui procurant ainsi un avantage injuste.
Trichage	Ensemble de principes moraux suivis par des personnes généralement considérées comme bonnes.



**10.** Pourquoi l'AMF est-elle utile ?

*c) Elle ajoute une couche supplémentaire de protection numérique.*

Compétences numériques — niveau intermédiaire

**11.** L'ergonomie, c'est :

*b) L'étude de l'environnement physique de travail des personnes.*

Compétences numériques — niveau intermédiaire

**12.** Placez un crochet (✓) pour toutes les suggestions qui peuvent vous aider à éviter l'inconfort ou les blessures lorsque vous travaillez avec de la technologie numérique.

Compétences numériques — niveau intermédiaire

Assurez-vous que vos genoux forment un angle de 90 degrés quand vous êtes assis.	✓
Utilisez toujours vos pouces pour taper des messages sur votre téléphone.	
Tenez votre téléphone sur vos genoux lorsque vous envoyez des textos.	
Faites régulièrement de courtes pauses lorsque vous travaillez à l'écran.	✓
Installez votre moniteur pour que le haut soit à la hauteur des yeux.	✓
Maintenez l'éclairage à un niveau élevé.	

**13.** La cyberchondrie, c'est :

*b) La crainte d'une maladie grave fondée sur des recherches de symptômes sur Internet.*

Compétences numériques — niveau intermédiaire



14.

Associez chaque exemple d'impact négatif possible d'un excès de technologie à une stratégie efficace pour réduire cet impact.

Compétences numériques — niveau intermédiaire

EXEMPLE	N° DE STRATÉGIE
Vous vivez de la cyberintimidation	4
Votre cou fait mal	3
Vous ne pouvez pas dormir	1
Vous vous sentez isolé	2

1. Arrêter le temps d'écran 30 minutes avant le coucher.
2. Planifiez une activité avec un ami de confiance en personne.
3. Surveillez la façon dont vous tenez votre téléphone.
4. Parlez-en à un adulte en qui vous avez confiance.

Quels sont vos résultats ?

Indiquez le nombre de réponses correctes. \_\_\_\_\_/14

11 — 14 réponses correctes : Bon travail ! Vous maîtrisez les principes de base et vos compétences pourraient augmenter assez rapidement avec de la pratique.

8 — 10 bonnes réponses : Continuez ! Vos compétences doivent être améliorées, mais certains éléments de base sont en place. Il est possible de s'améliorer assez rapidement.

< 7 : Vous avez vraiment besoin de vous exercer.