

INTELLIGENCE ARTIFICIELLE SÉCURITÉ ET CONFIDENTIALITÉ

Protégez vos données et utilisez l'intelligence artificielle en toute confiance

DESCRIPTION DE LA FORMATION

L'intelligence artificielle fait désormais partie de notre quotidien, tant dans la vie personnelle que professionnelle. Toutefois, son utilisation soulève des enjeux importants concernant la sécurité informatique, la confidentialité des renseignements, la protection des données personnelles et les risques de fraude.

Cette formation permet aux participants de comprendre les principaux risques associés à l'utilisation des outils d'intelligence artificielle et d'adopter des pratiques sécuritaires et responsables.

À travers des exemples concrets, des démonstrations et des exercices pratiques, les participants apprendront à protéger leurs renseignements personnels et professionnels, à reconnaître les menaces numériques et à utiliser les outils d'IA en toute confiance.

Cette formation s'adresse aux utilisateurs de l'intelligence artificielle et ne nécessite aucune connaissance en programmation.

OBJECTIFS DE LA FORMATION

À la fin de cette formation, les participants seront en mesure de :

- Comprendre les enjeux de sécurité et de confidentialité liés à l'intelligence artificielle.
- Reconnaître les risques associés au partage de renseignements personnels et professionnels.
- Protéger leurs données lorsqu'ils utilisent des assistants d'intelligence artificielle.
- Comprendre comment les informations transmises aux outils d'IA peuvent être utilisées et conservées.
- Identifier les tentatives de fraude, les contenus trompeurs et les cybermenaces utilisant l'IA.
- Configurer les principaux paramètres de confidentialité et de sécurité.
- Utiliser l'intelligence artificielle de façon responsable dans un environnement personnel ou professionnel.
- Adopter de bonnes pratiques pour prévenir les incidents de sécurité.

CLIENTÈLE

Cette formation s'adresse à toute personne souhaitant utiliser l'intelligence artificielle de manière sécuritaire et responsable, notamment :

- Les particuliers et les utilisateurs d'outils d'intelligence artificielle.
- Les employés et les professionnels de tous les secteurs.
- Les travailleurs autonomes et les entrepreneurs.
- Les gestionnaires et les responsables administratifs.

- Le personnel de soutien et de bureau.
- Les petites et moyennes entreprises (PME).
- Les organismes communautaires et les organismes sans but lucratif.
- Les personnes retraitées et les aînés utilisant les technologies numériques.
- Toute personne préoccupée par la confidentialité et la protection de ses renseignements.

CONTENU DE LA FORMATION

1. COMPRENDRE LES ENJEUX DE SÉCURITÉ LIÉS À L'INTELLIGENCE ARTIFICIELLE

- Introduction à la sécurité et à la confidentialité dans l'univers de l'IA.
- Différence entre sécurité informatique, confidentialité et protection des données.
- Pourquoi l'intelligence artificielle présente de nouveaux risques.
- Les renseignements personnels, confidentiels et sensibles.
- Les principales menaces liées aux outils d'intelligence artificielle.
- Les responsabilités des utilisateurs.
- Exemples concrets de situations à risque.

2. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET PROFESSIONNELS

- Identifier les renseignements qui doivent demeurer confidentiels.
- Comprendre les risques associés au partage de données avec une IA.
- Les informations à ne jamais transmettre à un assistant d'IA.
- Protection des coordonnées, documents d'identité et informations financières.
- Confidentialité des renseignements concernant les clients et les employés.
- Utilisation sécuritaire des documents professionnels.
- Techniques simples pour anonymiser les informations.
- Différence entre anonymisation et suppression des noms.
- Bonnes pratiques pour limiter la divulgation de renseignements sensibles.

3. CONFIDENTIALITÉ DES CONVERSATIONS AVEC LES ASSISTANTS D'IA

- Comprendre ce qui arrive aux informations transmises à une IA.
- Fonctionnement général de l'historique des conversations.
- Conservation et suppression des conversations.
- Différence entre mémoire, historique et utilisation des données pour améliorer les modèles.
- Comprendre les politiques de confidentialité des plateformes.
- Gestion des autorisations et du partage d'informations.
- Risques liés au téléchargement de fichiers confidentiels.
- Utilisation des conversations temporaires, lorsqu'elles sont disponibles.
- Vérification des paramètres de confidentialité.

- Atelier pratique :
 - Examiner les paramètres de confidentialité d'un assistant d'intelligence artificielle.

4. SÉCURISER SES COMPTES ET SES OUTILS D'INTELLIGENCE ARTIFICIELLE

- Création et gestion de mots de passe sécuritaires.
- Utilisation d'un gestionnaire de mots de passe.
- Authentification multifacteur et clés d'accès.
- Protection contre le vol de comptes.
- Reconnaître les faux sites et les applications frauduleuses.
- Vérifier la fiabilité d'un outil d'intelligence artificielle.
- Gestion des applications et des extensions de navigateur.
- Autorisations accordées aux outils connectés.
- Importance des mises à jour de sécurité.
- Utilisation sécuritaire de l'IA sur ordinateur, tablette et téléphone intelligent.

5. FRAUDES, HAMEÇONNAGE ET CYBERMENACES UTILISANT L'IA

- Comprendre comment les fraudeurs utilisent l'intelligence artificielle.
- Reconnaître les courriels et messages frauduleux.
- Hameçonnage personnalisé à l'aide de l'IA.
- Faux appels téléphoniques et imitation de voix.
- Usurpation d'identité numérique.
- Fraudes financières et demandes de paiement trompeuses.
- Faux profils et messages sur les réseaux sociaux.
- Reconnaître les signes d'une tentative de manipulation.
- Vérifier l'identité d'un interlocuteur.
- Mesures à prendre lorsqu'une fraude est soupçonnée.
- Atelier pratique :
 - Identifier les indices de fraude dans des courriels et des messages créés avec l'IA.

6. DEEPFAKES, FAUSSES INFORMATIONS ET MANIPULATION NUMÉRIQUE

- Comprendre ce qu'est un *deepfake* ou hypertrucage.
- Création de fausses images, vidéos et voix à l'aide de l'IA.
- Risques associés aux contenus artificiellement générés.
- Désinformation et manipulation de l'information.
- Comment vérifier la crédibilité d'une image ou d'une vidéo.
- Reconnaître les contenus suspects sans se fier uniquement à leur apparence.
- Vérification des sources d'information.
- Comprendre les limites des outils de détection de contenus générés par l'IA.
- Développer son esprit critique face aux contenus numériques.

7. UTILISATION SÉCURITAIRE DES DOCUMENTS ET DES FICHIERS

- Risques liés à l'importation de documents dans une plateforme d'IA.
- Protection des fichiers Word, Excel, PDF et autres documents.
- Utilisation sécuritaire des documents contenant des renseignements confidentiels.
- Suppression ou masquage des informations sensibles avant leur transmission.
- Risques associés aux fichiers provenant de sources inconnues.
- Vérification des documents produits par l'intelligence artificielle.
- Protection des données lors de l'analyse de fichiers.
- Précautions concernant les documents partagés et les espaces collaboratifs.
- Bonnes pratiques pour le stockage et la sauvegarde des fichiers.
- Atelier pratique :
 - Préparer un document afin de pouvoir l'utiliser avec une IA sans divulguer de renseignements confidentiels.

8. SÉCURITÉ DES OUTILS D'IA CONNECTÉS AUX APPLICATIONS

- Comprendre les connexions entre l'IA et les applications courantes.
- Autorisations d'accès aux courriels, calendriers et documents.
- Risques liés aux applications et services tiers.
- Comprendre les permissions accordées aux assistants d'IA.
- Protection des informations synchronisées.
- Risques liés aux automatisations et aux actions exécutées par l'IA.
- Comprendre les tentatives de manipulation des instructions d'un assistant.
- Vérifier les actions proposées avant leur exécution.
- Révoquer les accès devenus inutiles.
- Adopter une utilisation sécuritaire des assistants connectés.

9. INTELLIGENCE ARTIFICIELLE ET CONFIDENTIALITÉ EN ENTREPRISE

- Protection des renseignements appartenant à l'entreprise.
- Confidentialité des informations relatives aux clients et aux fournisseurs.
- Risques associés à l'utilisation d'outils d'IA personnels au travail.
- Différences entre les versions personnelles et professionnelles des plateformes.
- Respect des politiques internes de sécurité.
- Gestion des accès et des autorisations des employés.
- Protection des informations commerciales et stratégiques.
- Utilisation responsable de l'IA pour les courriels, rapports et documents.
- Validation des contenus générés avant leur diffusion.
- Importance d'une politique d'utilisation de l'intelligence artificielle en entreprise.

10. LOIS, RESPONSABILITÉS ET PROTECTION DE LA VIE PRIVÉE

- Principes fondamentaux de la protection des renseignements personnels.
- Présentation des principales obligations applicables au Québec et au Canada.

- Comprendre les principes essentiels de la Loi 25 au Québec.
- Consentement et utilisation des renseignements personnels.
- Responsabilités des organisations qui utilisent l'IA.
- Protection des renseignements concernant les employés et les clients.
- Transparence dans l'utilisation de l'intelligence artificielle.
- Respect de la vie privée et des droits des personnes.
- Importance de vérifier les obligations applicables à son organisation.

11. RISQUES ASSOCIÉS AUX RÉPONSES GÉNÉRÉES PAR L'IA

- Comprendre pourquoi une IA peut produire des informations erronées.
- Les hallucinations de l'intelligence artificielle.
- Risques liés aux recommandations inexactes.
- Vérification des faits et des sources.
- Précautions concernant les conseils médicaux, juridiques et financiers.
- Protection contre les décisions fondées uniquement sur une réponse d'IA.
- Reconnaître les biais et les informations trompeuses.
- Importance du jugement humain.
- Développer de bonnes habitudes de vérification.

12. BONNES PRATIQUES ET PRÉVENTION DES INCIDENTS

- Adopter une méthode sécuritaire avant de transmettre des informations.
- Vérifier les paramètres de confidentialité régulièrement.
- Limiter les renseignements partagés avec les outils d'IA.
- Choisir des plateformes reconnues et adaptées à ses besoins.
- Vérifier les autorisations des applications connectées.
- Éviter de transmettre des données confidentielles sans autorisation.
- Mettre en place des habitudes simples de cybersécurité.
- Savoir réagir lorsqu'une information confidentielle a été divulguée.
- Premières mesures à prendre en cas de compromission d'un compte.
- Signaler un incident à la personne ou au service responsable.
- Élaborer une liste personnelle de bonnes pratiques.
- Atelier pratique :
 - Élaborer sa propre liste de vérification pour une utilisation sécuritaire de l'intelligence artificielle.

RÉSULTATS ATTENDUS

À la fin de cette formation, les participants seront en mesure d'utiliser les outils d'intelligence artificielle de façon plus sécuritaire, de protéger leurs renseignements personnels et professionnels, de reconnaître les principales cybermenaces et d'adopter les bonnes pratiques nécessaires pour préserver leur confidentialité et leur vie privée.