MÉTIERS DU NUMÉRIQUE

Mise à jour : 23/07/2026

Cybersécurité et IA : adopter les bons réflexes pour protéger son entreprise

L'intelligence artificielle transforme les pratiques professionnelles mais également les méthodes des cybercriminels. Faux courriels, deepfakes, usurpation d'identité, rançongiciels ou vol de données : les attaques se multiplient et ciblent désormais en priorité les TPE, PME, collectivités et associations.

Cette formation apporte des solutions concrètes pour adopter les bons réflexes, sécuriser les usages numériques et intégrer l'IA comme un véritable outil de prévention au service de la sécurité de l'entreprise.

Dates
Sur demande, nous consulter

Durée
1 jour soit 7 heures - en présentiel

Tarifs
Pour un seul participant : 950 € - A partir de 2 participants : 500 €/participant

Possibilités de financement
OPCO selon branche d'activités

Lieux
Gap ou Briançon

Contact
Pascale STOUVENOT
06 33 65 65 61
p.stouvenot@cci05formation.fr

Référent Handicap
Aurélie THAVEAU
06 49 48 72 57
a.thaveau@cci05formation.fr

Modalités d'accès
Entretien téléphonique, puis inscription sur devis signé

Délai d'accès
Candidature à fournir avant le :
1 semaine avant

Blocs de compétences
Aucun

Équivalence
Aucune

Passerelles
Aucune

Suite de parcours
Aucune

Publics

Dirigeants, responsables de service, collaborateurs, assistants administratifs, collectivités et associations.

Objectifs

Développer une culture de cybersécurité au sein de l'entreprise afin de prévenir les cyberattaques, protéger les données et utiliser l'intelligence artificielle de manière responsable, sécurisée et conforme aux bonnes pratiques.

Pré-requis

Aucun

Programme

- Module 1 – Comprendre les nouvelles cybermenaces à l'ère de l'IA
- Module 2 – Sécuriser les usages numériques au quotidien
- Module 3 – Détecter et réagir face aux cyberattaques
- Module 4 – Construire son plan d'action cybersécurité

Matinée – Comprendre les cybermenaces et adopter les bons réflexes
Tour de table : pratiques numériques des participants, usages de l'IA et attentes.
Atelier : analyse de cyberattaques réelles ayant touché des TPE, PME et collectivités.
Mise en situation : reconnaître un phishing, un faux SMS, un QR Code frauduleux et un deepfake.
IA en pratique : utiliser ChatGPT pour analyser une tentative d'attaque et identifier les points de vigilance.
Exercices pratiques : renforcer la sécurité de ses mots de passe, de ses sauvegardes et de ses usages numériques.

Après-midi – Sécuriser son entreprise et construire son plan d'action
Diagnostic collectif : identifier les principales vulnérabilités de son entreprise.
IA en pratique : créer une check-list personnalisée des bonnes pratiques de cybersécurité.
Mise en pratique : élaborer des procédures simples en cas d'incident en cybersécurité et sensibiliser les collaborateurs.
Atelier collaboratif : construire un plan d'action cybersécurité priorisé selon les risques de son activité.
Bilan individuel : définir trois actions concrètes à mettre en oeuvre dès le retour en entreprise.

Moyens pédagogiques et techniques

Apports théoriques illustrés par des cyberattaques réelles ayant touché des entreprises françaises.
Démonstrations et analyses de situations concrètes.
Exercices pratiques de détection de tentatives de fraude (phishing, faux SMS, QR Codes frauduleux, deepfakes...).
Ateliers collaboratifs utilisant l'intelligence artificielle pour analyser les risques et construire des outils de prévention.
Élaboration d'un plan d'action personnalisé directement applicable dans l'entreprise.
Approche participative favorisant les échanges d'expériences et le partage de bonnes pratiques.

Minimum de 1 personne pour ouverture de session.

Accueil des stagiaires dans une salle dédiée à la formation. Documents supports de formation projetés.

Suivi et modalités d'évaluation

Évaluation diagnostique : recueil des pratiques, des usages numériques et des attentes des participants.
Évaluation formative : exercices pratiques, analyses de cas et mises en situation tout au long de la journée.
Évaluation finale : quiz de validation des acquis et présentation du plan d'action élaboré pendant la formation.
Auto-évaluation : identification des actions prioritaires à mettre en oeuvre dans son entreprise.

Livrables

À l'issue de la journée, chaque participant repart avec :
- Check-list des bonnes pratiques cybersécurité
- Guide "Utiliser l'IA sans mettre ses données en danger"
- Plan d'action personnalisé à 30 jours
- Fiche réflexe : "Que faire dans les 30 premières minutes après une cyberattaque ?"

Equipe pédagogique

Cette formation est animée par une consultante professionnelle, experte dans le domaine visé.

Débouchés

Non concerné

Les +

Formation orientée terrain, nombreux cas concrets issus des entreprises locales, utilisation raisonnée de l'IA comme outil de prévention, exercices de phishing et d'analyse de faux contenus générés par IA, ressources directement réutilisables dès le retour en entreprise.

Bénéfices pour les entreprises :
Réduire le risque de cyberattaque via IA.
Sensibiliser efficacement les collaborateurs.
Sécuriser les usages de l'intelligence artificielle.
Limiter les risques de fuite de données
Disposer d'un plan d'action immédiatement opérationnel.