

Sensibilisation à la cybersécurité pour collaborateurs - niveau 1

Comprendre et appliquer les bonnes pratiques de cybersécurité (mots de passe, phishing, RGPD) dans son quotidien professionnel

Durée : 7 heures dont 7 h avec formateur **EN PRESENTIEL** et 0 h en Digital Learning

Profils des apprenants : Tout collaborateur manipulant un ordinateur ou des données sensibles, télétravailleurs, managers, TPE/PME, associations, collectivités, grands groupes.

Prérequis : Niveau 1 | merci de bien prendre votre ordinateur pour la formation*

Points marquants :

- Pédagogie progressive : 50 % théorie, 50 % cas pratiques et simulations.
- Exercices de phishing en direct, quizz et mini-scénarios d'incident.
- Formateur certifié cybersécurité & RGPD – organisme Qualiopi.

Objectifs pédagogiques :

- Identifier les principaux risques en cybersécurité liés à l'utilisation de l'IA dans les environnements professionnels
- Comprendre le fonctionnement des cyberattaques ciblant les systèmes d'IA et les données qu'ils exploitent
- Adopter des comportements numériques sûrs pour sécuriser l'usage des outils d'IA en entreprise
- Mettre en œuvre les bonnes pratiques de gestion des données personnelles et sensibles dans des projets utilisant l'IA
- Renforcer la culture de cybersécurité au sein des équipes lors de l'intégration de solutions basées sur l'IA

Contenu de la formation :

- **Bloc de compétences : Bloc de compétences 1 : Comprendre les menaces et les enjeux de la cybersécurité**
 - Définir ce qu'est la cybersécurité et pourquoi elle est cruciale en entreprise
 - Comprendre les motivations et méthodes des cybercriminels
 - Identifier les principales menaces : phishing, malwares, ransomwares, ingénierie sociale
 - Expliquer les mécanismes des attaques par phishing et repérer les signes suspects
 - Prendre conscience de l'impact potentiel d'une attaque informatique pour l'entreprise
 - Analyser des cas concrets d'attaques réussies et en tirer des enseignements pratiques
 - Distinguer les différents types de malwares et leurs effets (spyware, virus, cheval de Troie, etc.)
 - Reconnaître les risques liés aux connexions en Wi-Fi public ou non sécurisé
 - Sensibiliser aux compétences managériales requises pour réagir face à une crise cyber
 - Expliquer la différence entre données personnelles et données sensibles selon le RGPD
 - Cas d'usage sur-mesure en fonction des demandes
- **Bloc de compétences : Bloc de compétences 2 : Adopter des comportements sûrs et responsables au travail**
 - Apprendre à gérer ses mots de passe : création, stockage et renouvellement sécurisé
 - Connaître les bonnes pratiques de navigation internet en entreprise
 - Maîtriser les usages sécurisés des e-mails professionnels et éviter les erreurs courantes
 - Prendre de bonnes habitudes dans la configuration et l'utilisation des outils numériques
 - Comprendre les risques liés aux périphériques amovibles (USB, disques durs externes, etc.)
 - Appliquer les règles de base de la cybersécurité sur les appareils mobiles et personnels
 - Adopter une posture proactive dans la déclaration des incidents et comportements suspects
 - Mettre en œuvre les grands principes du RGPD dans ses missions quotidiennes
 - Évaluer les risques liés aux réseaux sociaux et à la divulgation d'informations professionnelles
 - Encourager une culture collaborative de la cybersécurité au sein de l'équipe et de l'organisation
 - Cas d'usage sur-mesure en fonction des demandes



Organisation de la formation :

Equipe pédagogique :

Expert IA issu du monde de la cybersécurité

Moyens pédagogiques et techniques:

- Cours avec formateur en individualisant les besoins au sein d'un groupe
- Pour les formations dans nos locaux : salles de formation mises à disposition des stagiaires isolées du bruit, équipées d'ordinateurs portables, d'un vidéoprojecteur et d'un écran de TV géant. Nos locaux sont accessibles pour accueillir les personnes à mobilité réduite.
- Si la formation a lieu dans vos locaux, le lieu de formation mis à disposition devra être en adéquation avec la formation et avec une connexion internet
- Séances de formation en présentiel ou en distanciel (sur demande et par visio dans Teams avec un replay disponible)
- À la fin de chaque formation, chaque participant reçoit l'application IA avec le support de formation interactif
- Vous bénéficiez de 5 séances post-formation gratuite avec un expert IA sur les 12 mois après votre formation : **« Mon Club IA »**

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation :

- Questionnaire de positionnement en amont de la formation. Le programme est adapté et personnalisé, avant chaque session, nos experts font un tour de table afin de connaître les besoins des participants et orienter la formation en fonction de leurs attentes et les accompagner pour atteindre leurs objectifs.
- Nos formateurs Bonjour World adaptent une pédagogie très progressive en proposant aux apprenants des exercices pratiques qui leur sont remis et qui portent sur des cas concrets, tous les sujets sont ainsi traités. Ces exercices permettent un contrôle d'évaluation continu, de vérifier l'évolution des apprenants et de mesurer leurs acquis tout au long de la formation.
- Attestation individuelle de fin de formation.
- À l'issue de la formation, il sera remis à chaque personne formée un questionnaire de satisfaction et une attestation individuelle de fin de formation.
- Formation non certifiante mais un certificat de réalisation de formation sera livré à la fin de la formation en fonction de l'assiduité de l'apprenant

Accessibilité et délais d'accès :

Nos locaux sont accessibles pour accueillir les personnes à mobilité réduite. Notre Organisme de Formation et notre Référent Handicap, david@bonjour-world.com sont à votre écoute afin de permettre à chacun l'accès à nos formations. Une étude de vos besoins sera réalisée afin de construire et adapter votre formation en lien avec les experts mobilisables.

Pour accéder à cette formation, merci de contacter David Gesta au 02 38 21 51 52

Votre inscription pourra se faire minimum 48 heures avant la date de votre formation.

Dans le cadre d'un financement CPF, merci de prévoir 12 jours avant le début de la formation.

Prérequis matériel :

*Nous pouvons vous fournir un ordinateur portable si vous nous le demandez 1 semaine à l'avance

 ⚡ Prérequis matériel : venir avec votre ordinateur à la formation*. Pas besoin de compte payant ChatGPT mais si vous avez un compte, c'est encore mieux ! Nous ouvrons les comptes avec vous si vous le souhaitez ⚡

