CARHO
Conseil et Accompagnement en
Ressources Humaines & Orientation

Programme de la formation

« Cybersécurité – Niveau 1 - Utilisateurs »

ELEMENTS DE CONTEXTE

L'importance de la cybersécurité n'a jamais été aussi cruciale qu'aujourd'hui, surtout pour les petites et moyennes entreprises (TPE et PME). Ces entreprises, souvent moins bien protégées que les grandes organisations, sont devenues des cibles privilégiées pour les cyberattaques. Les conséquences d'une faille de sécurité peuvent être désastreuses, allant de la perte de données sensibles à des perturbations opérationnelles significatives et à des pertes financières.

FINALITE DE LA FORMATION

Renforcer les compétences en cybersécurité : Fournir aux dirigeants et employés de TPE et PME les connaissances et compétences nécessaires pour protéger leurs informations et leurs systèmes.

Prévenir les cybermenaces : Éduquer les participants sur les principales menaces de sécurité informatique et les stratégies pour les prévenir.

Mettre en place des pratiques sécurisées : Enseigner des pratiques et routines simples mais efficaces pour améliorer la sécurité informatique au quotidien.

Conformité réglementaire : Aider les entreprises à comprendre et à respecter les exigences légales et réglementaires en matière de protection des données.

OBJECTIFS PEDAGOGIQUES

Comprendre les bases de la sécurité informatique
Savoir maintenir ses outils à jour
Savoir sauvegarder ses données
Identifier les principales menaces
Savoir élaborer un plan de sécurité personnel

PUBLIC VISE

Tous les utilisateurs

- Dirigeants de TPE et PME : Pour qu'ils comprennent l'importance de la cybersécurité et puissent mettre en place des politiques de sécurité au sein de leur entreprise.
- Salariés : Ceux qui utilisent quotidiennement des systèmes informatiques et des données sensibles, afin de les sensibiliser aux risques et aux bonnes pratiques.

PRE-REQUIS

Personne ayant ou devant utiliser un outil informatique (PC, smartphone…)
Disposer d'un ordinateur portable
Disposer d'un ordinateur et du niveau minimal en informatique (savoir envoyer un mail, créer un compte GMAIL etc..)

DUREE

7h réparties sur une journée

TYPE
Formation en présentiel ou distanciel

MODALITES ET MOYENS PEDAGOGIQUES
Méthodes pédagogiques :
- Exposés théoriques
- Études de cas pratiques
- Ateliers et exercices interactifs
- Feedback et débriefing

Moyens pédagogiques :
- Support de formation (présentations, documents de référence).
- Vidéoprojecteur et tableau interactif pour les présentations.
- Outils de brainstorming et de travail collaboratif (post-it, paperboard, tableaux blancs).

Intervenant : Consultant expert en cybersécurité

EFFECTIF
Pour les formations en intra : de 2 à 12 participants par jour
Pour les formations en inter : de 4 à 12 participants par jour

DATES DES SESSIONS
Sessions établies selon la demande tout au long de l'année

TARIF
A partir de 450€ TTC par jour par personne. Pour les groupes importants, nous consulter.

MODALITES D'EVALUATION DE L'APPRECIATION DES STAGIAIRES
Evaluation sous forme de quiz ; Questionnaire d'évaluation de la satisfaction remis à chaque stagiaire en fin de formation ; Par mail, à l'entreprise avec la facture, envoi d'un certificat de réalisation dans les 30 jours qui suivent la fin de formation ainsi qu'un questionnaire de satisfaction entreprise adressé à + ou – 12 mois, afin d'évaluer l'impact de la formation dans l'organisation en place ; un questionnaire de satisfaction auprès des financeurs une fois par an en fin d'année civile ou début de l'année suivante.

SANCTION DE LA FORMATION
Une attestation de fin de formation est délivrée.

PERSONNE EN SITUATION DE HANDICAP
Nous compensons le handicap en formation en apportant des réponses individualisées et adaptées afin de rendre la prestation de formation « accessible » aux personnes handicapées. Pour toute inscription de personnes en situation de handicap, il convient de nous prévenir de manière à étudier les éventuels aménagements. La référente handicap à contacter est : Madame Elodie ALEYRAC – 04 68 78 22 01 – contact@carho.fr

CONTACTS ET INFORMATIONS
Tél. : 04.68.78.22.01 ou mail : contact@carho.fr
Elodie ALEYRAC : Responsable administrative, Assistante de direction
Caroline TRONC : Responsable pédagogique, Dirigeante de la SARL CARHO

MODALITES ET DELAIS D'ACCES (pour l'inscription)

Formation en intra ou en inter. La formation pourra être dispensée dès lors que le recueil du besoin client aura pu être établi suite à un échange physique, téléphonique ou mail ou suite à un diagnostic préalablement établi et lorsque la convention de formation sera datée et signée par les deux parties. Selon les disponibilités de l'organisme de formation, l'inscription peut se faire jusqu'à 15 jours calendaires avant le démarrage de la formation.

Programme détaillé

Matin	Après-midi
Comprendre les bases de la sécurité informatique - Les principales menaces : Virus, malwares, phishing - Exemples concrets de cyberattaques et leurs conséquences - Exemple de virus, ransomware et de phishing - Gestion des mots de passe : Pourquoi les mots de passe sont-ils cruciaux ? - Comment créer un mot de passe sécurisé : Méthode pour créer un mot de passe mémorable - Introduction aux gestionnaires de mots de passe *Atelier pratique : Créer et gérer des mots de passe sécurisés* **Savoir maintenir ses outils à jour** - Importance des mises à jour pour la sécurité *Atelier pratique : Vérifier et configurer les mises à jour sur les appareils*	**Savoir sauvegarder ses données** - Protéger ses données : Pourquoi sauvegarder ses données ? *Atelier Les méthodes simples de sauvegarde* - Introduction au chiffrement des données *Atelier pratique : Réaliser le chiffrement de données* **Identifier les principales menaces** - Sécurisation des communications : dangers des emails de phishing, comment les repérer ? - Bonnes pratiques pour les emails et la navigation internet *Atelier pratique : Reconnaître un email de phishing* - Utilisation sécurisée des appareils : sécuriser son smartphone et son ordinateur *Atelier pratique : Configurer les paramètres de sécurité sur les appareils* **Savoir élaborer un plan de sécurité personnel** - Importance de la sensibilisation et de la formation continue - Création de routines et de politiques de sécurité simples - Sécurité visuelle : Protéger ses informations en public *Atelier pratique : Élaborer un plan de sécurité personnel* *Évaluation : Quiz sur l'ensemble des points fondamentaux* **Synthèse et évaluation de la formation** - Retour sur les points clés de la formation. *Évaluation des acquis et du déroulement de la formation (questionnaires, discussion).* **Questions/Réponses et clôture** - Temps dédié aux questions des participants. *Conclusion du formateur et échange final*