

PROGRAMME DE FORMATION



Durée : 4h

Intra : 490 € HT par journée
10 pers. max

Inter : 140 € HT par journée
par personne

OBJECTIFS PÉDAGOGIQUES

Comprendre l'importance de la protection des données de l'entreprise
Savoir protéger son poste de travail informatique
Adopter les bonnes pratiques dans l'utilisation d'un système d'information
Savoir identifier les données vitales de son entreprise afin de les sauvegarder
Connaître les procédures à suivre en cas de cyberattaque

Public concerné

Nos formations s'adressent aux gérants, salariés ou indépendants souhaitant développer leurs compétences en informatique.

Prérequis

Maîtrise des compétences numériques de base.

Durée et tarif

La durée et les tarifs de la formation sont donnés à titre indicatif et pourront être adaptés en fonction des besoins identifiés et des modalités de mise en œuvre définies avec le bénéficiaire de la formation.

Délai d'accès

L'entrée en formation peut intervenir sous un délai moyen de 7 à 30 jours après validation administrative de votre dossier, selon les modalités de financement, et en fonction de vos besoins, préférences et contraintes.

Moyens matériels

Les apprenants évoluent :

- soit sur leur propre ordinateur, sous réserve qu'il réponde aux prérequis techniques de la formation
- soit sur un ordinateur portable mis à disposition par le centre de formation.

Pour les formations inter, une salle dédiée est mise à disposition, équipée d'un vidéoprojecteur et d'une connexion adaptée aux besoins des outils numériques utilisés.

Pour les formations intra, une validation préalable des matériels mis à disposition est nécessaire afin de s'assurer que l'environnement de formation est cohérent avec les objectifs pédagogiques et permet une mise en pratique immédiate des compétences visées.

Modalités pédagogiques

Les formations sont dispensées exclusivement en présentiel, en format inter-entreprises, intra-entreprise ou individuel. La méthode pédagogique alterne entre théorie et mise en pratique au travers d'exercices dirigés et de mises en situation. La finalité des formations aux outils informatiques est que l'apprenant soit capable d'utiliser la solution dans son environnement de travail quotidien et en totale autonomie.

Evaluation des compétences

L'évaluation des compétences repose sur un dispositif d'évaluation continue, intégré tout au long de la formation. Les acquis sont mesurés au travers d'exercices pratiques guidés, d'études de cas contextualisées, d'échanges techniques permettant de valider la compréhension et l'autonomie. La progression du participant est analysée tout au long du parcours afin d'adapter, si nécessaire, l'accompagnement et le rythme pédagogique.

Validation

Une attestation individuelle de formation sera remise à chaque participant sous condition que :

- Le participant a assisté à la totalité de l'action de formation
- Le formateur a validé la bonne acquisition des compétences abordées

Accessibilité

Les formations sont accessibles aux personnes en situation de handicap. Une étude des besoins spécifiques est réalisée afin d'adapter les modalités pédagogiques et organisationnelles si nécessaire.

1. Les enjeux de la cybersécurité

La cybersécurité, un sujet concret
Le cyberspace, nouvel espace de vie
Qui me menace et comment ?
Les différents types de menaces
Les conséquences d'une cyberattaque

2. Protéger son environnement

Comprendre le principe d'authentification
Choisir avec soin ses mots de passe
Sécuriser l'accès à son réseau Wi-Fi
Comprendre le rôle d'un antivirus
Télécharger ses logiciels sur des sites officiels
Mettre à jour régulièrement ses logiciels

3. Adopter les bonnes pratiques

Sécuriser ses mots de passe
Être prudent avec sa messagerie
Encadrer l'usage des supports amovibles

4. Séparer les usages

Comprendre le danger du mélange des usages

5. Anticiper le risque

Mettre en place une politique de sauvegarde
Que faire en cas d'incident ?

PROGRAMME DE FORMATION



Durée : 7h

Intra : 890 € HT par journée
10 pers. max

Inter : 245 € HT par journée
par personne

OBJECTIFS PÉDAGOGIQUES

Comprendre l'importance de la protection des données de l'entreprise
Savoir protéger son poste de travail informatique
Adopter les bonnes pratiques dans l'utilisation d'un système d'information
Savoir identifier les données vitales de son entreprise afin de les sauvegarder
Connaître les procédures à suivre en cas de cyberattaque

Public concerné

Nos formations s'adressent aux gérants, salariés ou indépendants souhaitant développer leurs compétences en informatique.

Prérequis

Maîtrise des compétences numériques de base.

Durée et tarif

La durée et les tarifs de la formation sont donnés à titre indicatif et pourront être adaptés en fonction des besoins identifiés et des modalités de mise en œuvre définies avec le bénéficiaire de la formation.

Délai d'accès

L'entrée en formation peut intervenir sous un délai moyen de 7 à 30 jours après validation administrative de votre dossier, selon les modalités de financement, et en fonction de vos besoins, préférences et contraintes.

Moyens matériels

Les apprenants évoluent :

- soit sur leur propre ordinateur, sous réserve qu'il réponde aux prérequis techniques de la formation
- soit sur un ordinateur portable mis à disposition par le centre de formation.

Pour les formations inter, une salle dédiée est mise à disposition, équipée d'un vidéoprojecteur et d'une connexion adaptée aux besoins des outils numériques utilisés.

Pour les formations intra, une validation préalable des matériels mis à disposition est nécessaire afin de s'assurer que l'environnement de formation est cohérent avec les objectifs pédagogiques et permet une mise en pratique immédiate des compétences visées.

Modalités pédagogiques

Les formations sont dispensées exclusivement en présentiel, en format inter-entreprises, intra-entreprise ou individuel. La méthode pédagogique alterne entre théorie et mise en pratique au travers d'exercices dirigés et de mises en situation. La finalité des formations aux outils informatiques est que l'apprenant soit capable d'utiliser la solution dans son environnement de travail quotidien et en totale autonomie.

Evaluation des compétences

L'évaluation des compétences repose sur un dispositif d'évaluation continue, intégré tout au long de la formation. Les acquis sont mesurés au travers d'exercices pratiques guidés, d'études de cas contextualisées, d'échanges techniques permettant de valider la compréhension et l'autonomie. La progression du participant est analysée tout au long du parcours afin d'adapter, si nécessaire, l'accompagnement et le rythme pédagogique.

Validation

Une attestation individuelle de formation sera remise à chaque participant sous condition que :

- Le participant a assisté à la totalité de l'action de formation
- Le formateur a validé la bonne acquisition des compétences abordées

Accessibilité

Les formations sont accessibles aux personnes en situation de handicap. Une étude des besoins spécifiques est réalisée afin d'adapter les modalités pédagogiques et organisationnelles si nécessaire.

1. Les enjeux de la cybersécurité

La cybersécurité, un sujet concret
Le cyberspace, nouvel espace de vie
Qui me menace et comment ?
Les différents types de menaces
Les conséquences d'une cyberattaque

2. Protéger son environnement

Comprendre le principe d'authentification
Choisir avec soin ses mots de passe
Identifier les différents utilisateurs
Sécuriser l'accès à son réseau Wi-Fi
Comprendre le rôle d'un antivirus
Télécharger ses logiciels sur des sites officiels
Mettre à jour régulièrement ses logiciels

3. Adopter les bonnes pratiques

Comprendre la navigation sur internet
Sécuriser ses mots de passe
Être prudent avec sa messagerie
Être vigilant lors d'un paiement en ligne
Se protéger du Social Engineering
Encadrer l'usage des supports amovibles
Protéger ses données lors d'un déplacement

4. Séparer les usages

Comprendre le danger du mélange des usages
Séparer les usages
Être aussi prudent avec son téléphone

5. Anticiper le risque

Identifier les données vitales
Mettre en place une politique de sauvegarde
Programmer un audit de sécurité
Anticiper la gestion de l'incident : PCA & PRA
Que faire en cas d'incident ?