





## Programme de la formation

### Cyberattaques : comment protéger mon business

-  Classe virtuelle
-  7 heures
-  Tout public · De 3 à 5 participants
-  490 € HT / 588 € TTC par participant

### Description courte

Cette formation fait partie du **PASS EXPERT : "Me spécialiser"** du [Passeport Formation](#).

**Cette formation est une première étape essentielle pour débutants en cybersécurité: Au cours de la journée, seront abordées les bonnes pratiques, socle indispensable à mettre en place avant d'aborder les outils informatiques, non inscrits au programme.**

### Profil des participants

- Consultants débutant en cybersécurité ne bénéficiant pas de la couverture d'un service informatique dans le cadre professionnel ou personnel, sans connaissances informatiques particulières autres que ce qui est demandé en pré-requis et voulant améliorer leur cybersécurité.

### Prérequis

- Disposer d'un ordinateur avec accès internet, son et webcam
- Etre à l'aise en connexion à distance
- Un deuxième écran est conseillé pour le confort des participants

### Objectifs

- Inventorier et comprendre les principaux types de cyberattaque
- Reconnaître ces cyberattaques
- Identifier et acquérir les bonnes pratiques d'hygiène informatique permettant d'éviter ou de minimiser l'impact des cyberattaques.
- Mettre en œuvre ces pratiques sur son matériel informatique actuel.

### Aptitudes et compétences visées / attestées

- Etre en mesure de repérer des cyberattaques et de les éviter ou de les minimiser en appliquant des bonnes pratiques d'hygiène informatique. Et par cela, sécuriser son business, ses données et sa réputation vis-à-vis de sa clientèle.

### Contenu

I- Accueil du groupe



## II- Principales cyberattaques à connaître.

### III- Etude des bonnes pratiques

1. Protéger ses données, ne pas mélanger pro/perso
2. Définir des mots de passe et identifications robustes
3. Sécuriser ses applications mobile
4. Naviguer en sécurité
5. Verrouiller l'utilisation des courriels
6. Spécificités avec le téléphone

### IV- Contrer les cyberattaques

## Pédagogie et organisation

- Méthodes pédagogiques
  - En amont des visio-formations, demande d'un auto-diagnostic, et initiation d'une réflexion sur les sauvegardes pour renforcer l'engagement des participants et rendre la visio-formation plus efficace.
  - Techniques d'animation interactives adaptées aux classes virtuelles
  - Les participants sont très sollicités afin de leur permettre de s'approprier pleinement le contenu de la formation et de le mettre en pratique au quotidien.
  - Exemples et exercices concrets, partage d'expérience, co-construction d'une synthèse
- Matériel pédagogique :
  - Ordinateur, outil de visio-formation, outils digitaux de préparation et d'animation
  - Support de cours, et lexique des termes utilisés en mode numérique..

## Positionnement et Modalités d'évaluation des acquis

- **Test de positionnement en amont** : questionnaire à renvoyer avant la formation
- **Evaluation des acquis /compétences liées aux objectifs opérationnels définis** :

Connaissances ou compétences	Modalités d'évaluation (QUIZZ, exercices...)	Critères d'évaluation (%de réussite, ou comparaison entrée et sortie de stage...)	
Inventorier et comprendre les principales menaces	Quizz	70% réussite	
Reconnaitre ces cyberattaques	Exercice sur courriel piégé, tableau	Tableau rempli en mode collaboratif	
Identifier et acquérir les bonnes pratiques d'hygiène informatique	Exercice : tableau de synthèse	Rempli en mode collaboratif	



- Fiche d'évaluation qualitative de la formation à chaud

## Mode de validation

Attestation de fin de formation

## Modalités et délai d'accès

- Lieu de la formation et accès : en visio-formation Zoom, lien diffusé par l'adresse mail.
- Conditions d'accueil: avoir une connexion internet et télécharger l'application Zoom.
- Délais d'inscription : au minimum 10 jours avant le démarrage de la visio-formation.

## Référent handicap

**PERSONNES EN SITUATION DE HANDICAP :** (*mise en place de compensation...*)

**Contact :** Référent handicap 02 51 84 95 55 / 06 28 70 45 28 / [nadiahadjeri@cadresenmission.com](mailto:nadiahadjeri@cadresenmission.com)

## Intervenant

- Thierry Hamon, consultant cash management et cybersécurité en portage salarial depuis 2016
- Ancien auditeur PriceWaterhouseCoopers, ancien responsable informatique de la C.O.F.F.R.A.
- Cours de cybersécurité au Luxembourg pour trésoriers chez House of Training, conférences
- Certification LinkedIn CompTIA Security+ (SY0-601) Menaces, attaques et vulnérabilités

## Prochaines sessions

Le 22/06/2026 à distance Le 14/09/2026 à distance Le 14/10/2026 à distance

## Évaluations

50 inscriptions depuis le 13/10/2023

**Taux d'acquisition des compétences :**  **91 %** (49 évaluations)

**Satisfaction des apprenants :**  **4.4/5** (49 évaluations)