



# FORMATION CYBERSÉCURITÉ

## Les essentiels de la Cybersécurité



## Formation réalisée en Réalité Virtuelle

### OBJECTIF DE LA FORMATION

**Maîtriser les techniques de la cybersécurité afin d'éviter à vous et vos collaborateurs de tomber dans les pièges des cyberattaques.**

85 % des violations de la cybersécurité sont causées par une erreur humaine. Vivez une cyberattaque pour comprendre les enjeux autour de la cybersécurité. Apprenez à identifier les risques et à adopter les bons réflexes pour favoriser la sécurité.

**À l'issu de ce parcours, vous serez capable de :**

- Identifier et éliminer les éléments malveillants
- Adopter les bonnes pratiques en cybersécurité
- Réagir efficacement en cas d'attaque cybercriminelle

### CONTENU

- Les enjeux de la formation
- La détection des emails malveillants
- La sécurité des comptes et mots de passe
- La conservation des mots de passe
- Les actions face à un acte cybercriminel

## PRÉ-REQUIS

- Aucun pré requis

## PUBLIC VISÉ

- La formation s'adresse à tout public désirant se sensibiliser à la cybersécurité

## MODALITÉS D'ADMISSION

Aucune.

## MODALITÉS PÉDAGOGIQUES

- Simulations et immersion dans des scénarios interactifs afin d'assurer l'acquisition de bons réflexes grâce à l'entraînement et la pratique
- Débriefing avec un/une coach avec identification des forces et des axes d'amélioration
- Évaluation en fin de formation
- Complément d'apports théoriques avec le formateur
- + Accès pendant 2 mois illimité à la plateforme de cours - 24h/24 et 7j/7 pour davantage de théorie et de rappels fréquents

## LOCALISATION & ACCESSIBILITÉ

- Nous formons en présentiel et en visioconférence sur toute la France
- Nos méthodes pédagogiques et nos modalités d'évaluation sont adaptables au public en situation de handicap

## DURÉE DE LA FORMATION

- À déterminer selon les besoins
- Planification des modalités de formation à définir avec l'entreprise ou le(s) stagiaire(s)

## En fin de stage :

Questionnaire « qualité » à remplir par tous les stagiaires.

Questionnaire qualité remis au donneur d'ordre.

## QCM et Évaluation

→ Remise d'un certificat de réalisation attestant l'acquisition des compétences attendues

→ Remise d'une attestation de formation attestant l'acquisition des compétences attendues

---

## PROGRAMME DE FORMATION

---

### MODULE

Les essentiels de la cybersécurité

## THÈME 1 : Les enjeux de la formation

### Contenu du thème :

- Découvrez les enjeux liés aux emails malveillants pour les entreprises
- Mise en situation

## THÈME 2 : La détection des emails malveillants

### Contenu du thème :

- Apprenez à décomposer un email malveillant et les zones sur lesquelles il faut être vigilant
- Mise en situation

## THÈME 3 : La sécurité des comptes et mots de passe

### Contenu du thème :

- Comprenez l'importance de sécuriser ses comptes et mots de passe à travers l'expérience d'un collaborateur
- Mise en situation

## THÈME 4 : La conservation des mots de passe

### Contenu du thème :

- Apprenez les bonnes pratiques pour conserver vos mots de passe et sécuriser vos connexions
- Mise en situation

## THÈME 5 : Les actions face à un acte cybercriminel

### Contenu du thème :

- Réagissez efficacement en cas d'attaque cybercriminelle à travers l'expérience d'une collaboratrice
- Mise en situation

## THÈME 6 : Évaluation et bilan

### Contenu du thème :

- Mémorisez l'essentiel de cette formation
- Testez vos connaissances en répondant à des questions clés et débriefez avec le formateur.

---

# INFORMATIONS COMPLÉMENTAIRES

---

## DÉLAI D'ACCÈS

Le délai d'accès à la formation est de 2 à 3 semaines après validation de votre dossier.

Planification des modalités de formation à définir avec l'entreprise ou le(s) stagiaire(s).

## MODALITÉS DE FINANCEMENT

→ Autofinancement

→ OPCO

→ La Région

→ Pôle Emploi

→ L'entreprise

## TARIFS (SUR DEVIS)



[infos@afformation.fr](mailto:infos@afformation.fr)

04 51 00 93 51

---