Sensibilisation à la Cybersécurité

Protégez vos Données et Votre Vie Numérique

Présentation

Cette formation présente l’importance de la cybersécurité à l'ère du numérique. Elle souligne les risques auxquels les individus et les organisations sont confrontés, et l'importance d'une sensibilisation accrue dans la prévention des attaques.

La formation de sensibilisation à la cybersécurité est un excellent moyen de se protéger des cyberattaques. Elle permet aux participants d'acquérir les connaissances et les compétences nécessaires pour se protéger de manière efficace.

Public cible

La formation de sensibilisation à la cybersécurité est destinée à un large public, des particuliers aux professionnels. Elle est particulièrement recommandée pour les personnes qui utilisent des outils numériques dans leur vie personnelle ou professionnelle (employés d'entreprise, des étudiants, des particuliers ou d'autres groupes.)
Avec un effectif de 10 à 20 apprenants.

Prérequis

Posséder un ordinateur et un accès internet. Savoir lire, écrire et se connecter à internet.

Objectifs pédagogique

- Être sensibilisé sur les concepts de sécurité et de sauvegarde en entreprise et dans la vie privée..
- Renforcer la sensibilisation des participants aux risques liés à la cybersécurité.
- Fournir aux participants les connaissances et les compétences nécessaires pour se protéger contre les cyberattaques.
- Encourager les participants à adopter des comportements sûrs en ligne.

Compétences visées

Sensibiliser les participants aux risques de faille de sécurité informatique
Apprendre aux participants les bonnes pratiques pour se protéger
Développer une attitude de vigilance et de prévention chez les participants
Comprendre les menaces courantes en ligne.
Être capable de reconnaître les signes d'attaques potentielles sur ordinateur.

Durée

La durée de la formation est de 14 heures

Suivi pédagogique

La formation par l'équipe pédagogique composé de Claudith experte en cybersécurité,olivier programmeur et de David expert en cybersécurité

Equipe pédagogique est aussi sur discord et la communauté des apprenants.

Modalités pédagogique

Les modalités pédagogiques de la sensibilisation à la cybersécurité sont les suivantes :

- **L' information** : il s'agit de fournir aux participants les connaissances et les informations nécessaires pour comprendre les risques en cybersécurité. Cette

information peut être dispensée sous forme de présentations, de documents, de vidéos ou de simulations.
- **La formation** : il s'agit d'apprendre aux participants à mettre en place des mesures de cybersécurité pour se protéger. Cette formation peut être dispensée sous forme de cours, de tutoriels ou d'exercices pratiques.
- **La sensibilisation** : il s'agit de faire prendre conscience aux participants de l'importance de la cybersécurité et de leur responsabilité dans la protection de leurs données. Cette sensibilisation peut être réalisée par des campagnes de communication, des jeux concours ou des témoignages.
- La formation est interactive et participative. Elle utilise une variété de **méthodes pédagogiques**, notamment :
    - Des présentations PowerPoint
    - Des exercices pratiques
    - Des discussions en groupe

Modalités d’évaluation

Les modalités d'évaluation de la sensibilisation à la cybersécurité peuvent être classées en deux catégories :

- **Questionnaires** : les questionnaires sont un moyen simple et efficace d'évaluer les connaissances et les compétences des participants. Ils peuvent être administrés en ligne ou en présentiel.
- **Exercices pratiques** : les exercices pratiques permettent aux participants de mettre en application les connaissances acquises. Ils peuvent être réalisés en individuel ou en groupe.
- **Simulations d'attaques** : les simulations d'attaques permettent aux participants de tester leurs compétences en cybersécurité dans un environnement sécurisé.
- **Entretiens individuels** : les entretiens individuels permettent au formateur d'obtenir un feedback plus approfondi sur les connaissances et les compétences des participants.

Modalités de certification visés

Attestation de sensibilisation aux gestes et comportements sécurisés dans le cyberespace.

Lieux

La formation se déroule au 123 avenue des champs Elysées 75001 PARIS de 9h00 à 18h00

Tarif

Le prix du forfait de la prestation est de 1200 € TTC pour les deux jours
Les modalités de paiements sont sur le contrat ou CGV

Moyens matériel

- **Présentations** : les présentations sont un moyen efficace de transmettre des informations sur la cybersécurité. Elles peuvent être utilisées pour expliquer les concepts de base de la cybersécurité, les menaces et les risques, et les mesures de protection.
- **Vidéos** : les vidéos sont un moyen attrayant et engageant de transmettre des informations sur la cybersécurité. Elles peuvent être utilisées pour illustrer les concepts de cybersécurité, les menaces et les risques, et les mesures de protection.
- **Documents** : les documents, tels que les guides pratiques, les brochures et les articles, sont un moyen efficace de fournir des informations sur la cybersécurité. Ils peuvent être utilisés pour fournir des informations plus détaillées sur les concepts de cybersécurité, les menaces et les risques, et les mesures de protection.
- **Jeux et simulations** : les jeux et les simulations sont un moyen interactif et engageant de sensibiliser à la cybersécurité. Ils peuvent être utilisés pour tester les connaissances et les compétences des participants en matière de cybersécurité.

Poursuite en formation

La cybersécurité est un domaine en constante évolution, et les professionnels de la cybersécurité doivent être prêts à apprendre et à évoluer au fur et à mesure que les menaces et les technologies évoluent.

Il existe de nombreuses possibilités de poursuite en formation après la cybersécurité. Ces formations peuvent permettre aux professionnels de la cybersécurité de se spécialiser dans un domaine particulier, d'acquérir de nouvelles compétences ou de se préparer à des postes de direction.

Voici quelques exemples de poursuites en formation possibles après la cybersécurité :

- **Master en cybersécurité** : ce type de master permet aux professionnels de la cybersécurité d'acquérir des connaissances et des compétences avancées dans un domaine particulier de la cybersécurité, comme la sécurité des réseaux, la sécurité des applications ou la sécurité des données.
- **Certifications** : les certifications sont un moyen de démontrer ses compétences et ses connaissances en cybersécurité. Il existe de nombreuses certifications disponibles, correspondant à différents niveaux d'expertise.
- **Formations en ligne** : les formations en ligne offrent une flexibilité importante et permettent aux professionnels de la cybersécurité de se former à leur rythme. Il existe de nombreuses formations en ligne disponibles, couvrant un large éventail de sujets.

Délai d'accès

Durée de mise à disposition par le Centre de Formation ou le Formateur de la formation, disponible sous 14 jours de délai minimum.

Accessibilité et handicap

Pour toutes nos formations, nous réalisons des études préalables à la formation pour adapter les locaux, les modalités pédagogiques et l'animation de la formation en fonction de la situation de handicap annoncée. De plus, en fonction des demandes, nous mettrons tout en œuvre pour nous tourner vers les partenaires spécialisés.

Notre Référent Handicap : M. David KRIEF , 6 rue de la Saône, 78310 MAUREPAS

Témoignage et évaluation de la formation

Mise à disposition de formulaires d'évaluation de la formations à la fin de la formation puis à 3 mois pour un suivi d'activité et évaluer leurs nouvelles compétences

Témoignage apprenant/commanditaire

Listes des clients éventuels et des témoignages comme gage de qualité

Programme pédagogique/Modalités pédagogiques

Jour 1

- Matinée
    - Présentation des concepts fondamentaux de la cybersécurité
    - Définition des menaces et des vulnérabilités
- Après-midi
    - Identification des menaces et des vulnérabilités
    - Mise en place de mesures de protection

Jour 2

- Matinée
    - Bonnes pratiques en ligne
    - Bonnes pratiques en matière de sécurité des données
- Après-midi
    - Exercices pratiques
    - Discussion avec un formateur