

FICHE DE FORMATION PROFESSIONNELLE

(Plan de formation)

Cette fiche ou plan de formation est susceptible d'être enrichi progressivement afin de vous offrir des formations toujours plus complètes et de qualité.

Sécurité Informatique

Initiation à la Cybersécurité : Niveau Débutant

Sous-titre : Adopter les bonnes pratiques pour sécuriser son environnement numérique personnel et professionnel

AVERTISSEMENT

Ni le formateur Ni IT Expert ne sont responsables de la mauvaise utilisation du contenu de cette formation. L'utilisation des outils doit être réalisée uniquement au sein d'un environnement virtuel ou avec une autorisation préalable.

Option 1 : Professionnelle et Juridique (Recommandée)

CLAUDE DE NON-RESPONSABILITÉ Le formateur et l'entité IT Expert déclinent toute responsabilité quant aux conséquences d'une utilisation malveillante ou inappropriée du contenu de cette formation. L'usage des outils et techniques présentés doit impérativement s'effectuer dans un cadre légal, au sein d'un laboratoire virtuel isolé ou avec le consentement écrit des parties concernées.

Option 2 : Pédagogique et Directe

AVERTISSEMENT ÉTHIQUE Ce cours est destiné à un usage strictement éducatif. Le formateur et IT Expert ne pourront être tenus responsables des dommages résultant d'un mauvais usage de ces connaissances. Nous rappelons que toute expérimentation technique doit être limitée à un environnement de test sécurisé ou faire l'objet d'une autorisation préalable explicite.

Option 3 : Concise (Format "Fiche Résumé")

IMPORTANT : Le formateur et IT Expert ne sauraient être tenus responsables de l'usage fait des informations transmises. L'utilisation des outils de sécurité est soumise au respect de la loi

: utilisez exclusivement des environnements virtuels ou assurez-vous d'avoir une autorisation préalable.

Option 4 : Style "Hacker Éthique"

CADRE D'UTILISATION : La maîtrise des outils de sécurité implique une grande responsabilité. Ni le formateur, ni IT Expert ne sont responsables des actions des apprenants. Toute pratique hors d'un environnement virtuel dédié ou sans accord préalable est strictement interdite et peut être passible de sanctions pénales.

1 Présentation de la formation

La transformation numérique expose de plus en plus les particuliers, entreprises et institutions aux menaces informatiques. Cette formation d'initiation à la cybersécurité a pour objectif de doter les apprenants des **fondamentaux essentiels** pour comprendre les risques numériques actuels et adopter des **comportements sécurisés** au quotidien.

Conçue selon une approche pédagogique progressive, elle ne nécessite **aucune connaissance technique préalable** et met l'accent sur les **bonnes pratiques opérationnelles**, immédiatement applicables.

2 Objectifs pédagogiques

À l'issue de la formation, l'apprenant sera capable de :

- Identifier les principales menaces de cybersécurité (phishing, ransomware, ingénierie sociale, logiciels malveillants).
- Comprendre les mécanismes utilisés par les cybercriminels pour exploiter les failles humaines.
- Sécuriser ses comptes numériques grâce à des méthodes d'authentification robustes.
- Appliquer les règles d'hygiène numérique sur un poste de travail personnel ou professionnel.
- Utiliser Internet de manière sécurisée.
- Réagir efficacement face à une tentative ou un incident de sécurité informatique.

3 Compétences acquises

À la fin de la formation, l'apprenant saura :

- Mettre en place des mots de passe forts et une authentification multifacteur (MFA).
- Reconnaître et éviter les tentatives de phishing et d'arnaques en ligne.
- Sécuriser ses données par des sauvegardes fiables.
- Adopter un comportement responsable et sécurisé dans l'usage des outils numériques.
- Appliquer une procédure simple en cas de suspicion de piratage.

4 Public concerné

- Salariés d'entreprises et d'administrations
- Étudiants et élèves
- Entrepreneurs, indépendants et dirigeants de PME
- Toute personne utilisant des outils numériques et souhaitant renforcer sa sécurité informatique
- Toute personne souhaitant se former

5 Prérequis

- Savoir utiliser un ordinateur (Windows ou macOS)

- Savoir naviguer sur Internet
- Volonté d'apprendre et d'innover

👉 **Aucune connaissance technique en informatique ou en réseau n'est exigée**

6 **Durée et organisation**

- **Durée totale** : 3 Mois
- **Organisation possible** :
 - 4 sessions de 3 heures
 - ou 6 sessions de 2 heures
- **Rythme** : Flexible
- **Date de début** : Flexible

7 **Table des matières (Sommaire)**

MODULE 1 – Les Bases de la Confiance Numérique

Objectif : Comprendre l'évolution de la menace et les principes fondamentaux de protection (Modèle CIA).

- **Chapitre 1 : Introduction et Histoire**
 - Définition de la cybersécurité et enjeux mondiaux.
 - Histoire : Des premiers virus aux cyberguerres modernes.
 - L'économie du cybercrime : Pourquoi tout le monde est une cible.
- **Chapitre 2 : La Triade de la Sécurité (CIA)**
 - Confidentialité, Intégrité et Disponibilité en profondeur.
 - Le concept de "Défense en profondeur" (Le modèle de l'oignon).
- **Chapitre 3 : Le Vocabulaire du Risque**
 - Comprendre le trio : Menace, Vulnérabilité et Impact.
 - Terminologies essentielles pour le débutant.

Quiz du Module 1

MODULE 2 – Le Bestiaire des Menaces (Le paysage des risques)

Objectif : Identifier les dangers, les types d'attaquants et leurs méthodes de prédilection.

- **Chapitre 1 : Les Logiciels Malveillants (Malwares)**
 - Virus, Vers, Chevaux de Troie et Spywares.
 - Ransomwares : Fonctionnement et économie des rançons.
- **Chapitre 2 : L'Ingénierie Sociale (Le Hack Humain)**
 - Phishing, Smishing et Vishing : Détecter les pièges.
 - Psychologie de l'attaque : Comment les émotions sont manipulées.
- **Chapitre 3 : Anatomie d'une Cyberattaque**
 - Qui sont les hackers ? (Black Hat, White Hat, État-nations).
 - Les phases de l'attaque : De la reconnaissance à l'action.

Quiz du Module 2

MODULE 3 – Sécuriser son Espace de Travail

Objectif : Appliquer l'hygiène numérique sur ses appareils et gérer ses identités.

- **Chapitre 1 : La Forteresse des Accès (IAM)**
 - Anatomie d'un mot de passe robuste et gestionnaires de mots de passe.
 - L'Authentification Multi-Facteurs (MFA/2FA) : La barrière ultime.
- **Chapitre 2 : Sécurité des Systèmes et Appareils**
 - Windows, Linux, macOS : Sécurité comparée et mises à jour.

- Antivirus, Pare-feu et protection des objets connectés (IoT).
- **Chapitre 3 : Mobilité et Travail Nomade**
 - Sécuriser son smartphone (iOS/Android).
 - Les bonnes pratiques du télétravail.

Quiz du Module 3

MODULE 4 – Réseaux et Protection des Données

Objectif : Comprendre comment circulent les données et comment les verrouiller.

- **Chapitre 1 : Les Bases du Réseau Sécurisé**
 - Comment fonctionne Internet ? (Modèle OSI simplifié, IP, DNS).
 - Sécuriser sa Box Internet et son Wi-Fi (WPA2/WPA3).
- **Chapitre 2 : Cryptographie pour Débutants**
 - Chiffrement symétrique vs asymétrique.
 - Le protocole HTTPS et l'utilité réelle d'un VPN.
- **Chapitre 3 : Sauvegardes et Supports Physiques**
 - Sécuriser ses données : La règle du 3-2-1.
 - Dangers des supports amovibles (Clés USB, disques externes).

Quiz du Module 4

MODULE 5 – Droit, Éthique et Réaction

Objectif : Connaître le cadre légal et savoir réagir face à un incident.

- **Chapitre 1 : Protection des Données et Vie Privée**
 - Introduction au RGPD et responsabilités légales.
 - Confidentialité des données en entreprise.
- **Chapitre 2 : Le Hacking Éthique et Carrières**
 - Tester pour mieux protéger : Méthodologies de base.
 - Panorama des métiers de la cybersécurité.
- **Chapitre 3 : Gestion des Incidents (Le Plan d'Urgence)**
 - Procédure simple en cas de suspicion de piratage.
 - Continuité d'activité : Comment redémarrer après une attaque.

Quiz du Module 5

MODULE 6 – Pratique, Études de Cas et Ressources

Objectif : Valider les acquis par l'analyse de situations réelles.

- **Études de Cas :** Analyses pédagogiques de piratages célèbres (ex: WannaCry, Fraude au Président).
- **Examen Final :** Grand QCM de validation des 5 compétences clés.
- **Annexes :**
 - Glossaire complet de la cybersécurité.
 - Fiches résumés "Réflexes de survie".
 - Liste d'outils et ressources pour aller plus loin.

8 Méthodes pédagogiques

- Exposés interactifs
- Études de cas réels
- Démonstrations pratiques
- Simulations de phishing
- Quiz et exercices d'application
- Échanges et retours d'expérience

9 Modalités d'évaluation

- Quiz de validation des connaissances
- Exercices pratiques
- Participation active aux sessions

10 Validation de la formation

- **Attestation de fin de formation** délivrée au participant

1 1 Modalités de formation

- **Format** : En ligne
- **Supports** :
 - PDF
 - Vidéo
 - **Check-lists de sécurité**
 - Ressources complémentaires

1 2 Débouchés et utilité professionnelle

Cette formation permet de :

- Réduire les risques d'incidents informatiques
- Améliorer la sécurité numérique individuelle et collective
- Renforcer la culture cybersécurité en entreprise ou institution
- Constituer une base solide pour des formations de niveau intermédiaire et avancé

✓ Formation idéale comme :

- Module d'initiation
 - Sensibilisation en entreprise
 - Prérequis à une formation avancée en cybersécurité
-

Ne manquez pas votre chance d'évoluer

La solution est ici. Ne laissez pas vos compétences actuelles freiner votre carrière.

Inscrivez-vous maintenant et commencez votre transformation professionnelle aujourd'hui.