CYBERSÉCURITÉ EN SANTÉ

DURÉE : **11H**

Document mis à jour en janvier 2024

DPC | E-LEARNING

PROGRAMME INTÉGRÉ

6H ÉVALUATION DES PRATIQUES PROFESSIONNELLES

5H FORMATION CONTINUE

0€ RESTE À CHARGE

INDEMNISATION **495€**

PRIX : 978.5€ 100% FINANCÉ

NUMÉRO D'ACTION :
96592325113

INTERVENANTE
DIRECTRICE GÉNÉRALE CYBERWINGS, INGÉNIEURE EN SYSTÈMES D'INFORMATION ET CONSULTANTE EN CYBERSÉCURITÉ

PUBLIC CIBLÉ
MÉDECINS GÉNÉRALISTES

> RÉSUMÉ DE LA FORMATION

Hôpitaux, cliniques, laboratoires d'analyse, cabinets médicaux, etc… sont des organisations de plus en plus **ciblées par les cybercriminels.**

Cette sensibilisation vous permettra **d'appréhender les différents moyens utilisés** par les attaquants pour exploiter les vulnérabilités de votre système d'information et compromettre ainsi les données sensibles.

Vous comprendrez ainsi pourquoi le secteur de la santé est particulièrement visé et connaîtrez les **principaux gestes à pratiquer** au quotidien pour protéger les données numériques que vous manipulez (hygiène numérique).

Cette formation s'inscrit dans le cadre d'un **programme intégré** en s'articulant sur la **formation continue** ainsi que sur l'**évaluation des pratiques professionnelles** (EPP).
La méthode utilisée pour l'évaluation de pratiques professionnelles est celle de **l'audit clinique.**

> OBJECTIFS OPÉRATIONNELS

Concevoir et maintenir sécurisé son environnement numérique de travail.

Savoir se prémunir et réagir face aux incidents.

Adopter une bonne hygiène numérique.

Analyser sa pratique professionnelle.

OBJECTIFS OPÉRATIONNELS - SUITE

A l'issue de la formation, les participants seront en capacité de :

Connaître les cyberattaques et la sécurité des systèmes d'information.
Protéger leurs données par une authentification forte.
Adopter les bonnes pratiques en situation de mobilité et de télétravail.
Se prémunir contre le phishing et social engineering.
Mettre en œuvre une hygiène numérique au quotidien.

DÉROULÉ DU PARCOURS DE FORMATION

MODULE 01 — PRENDRE CONNAISSANCE DES RECOMMANDATIONS

Prendre connaissance des référentiels en cybersécurité :

- Référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux – Commission Nationale de l'Informatique et des Libertés (CNIL), 28 juillet 2020.
- Politique Générale de Sécurité des Systèmes d'Information (PGSSI).
- Le Guide d'hygiène informatique de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

MODULE 02 — CONTEXTE DE LA CYBERSÉCURITÉ EN SANTÉ

Qu'est-ce que la Sécurité des Systèmes d'Information (SSI), notion de DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité).
Actualité des attaques en santé.
Quels sont les impacts suite à une cyber-attaque ?
Physionomie de la cyber-criminalité.
Comment se déroule une attaque ?
Le contexte réglementaire de la sécurité lié à la santé.
Les différents référentiels de la sécurité numériques (PGSSI, ANSSI et CNIL).
Les organismes de sécurité numérique liés à la santé à connaître.
L'organisation de la Sécurité des Systèmes d'Information (SSI).
Pourquoi il est important d'avoir une bonne hygiène numérique malgré les technologies de protection ?

MODULE 03 — L'IMPORTANCE DE L'AUTHENTIFICATION

Qu'est-ce que l'authentification ?
Pourquoi des droits d'accès différents sur les applications ?
Les attaques les plus courantes : fuites des mots de passe, création de dictionnaires des mots de passe les plus courants, prêt du mot de passe, diffusion du mot de passe.

DÉROULÉ DU PARCOURS DE FORMATION - SUITE

MODULE 03 - SUITE	L'IMPORTANCE DE L'AUTHENTIFICATION

Votre adresse mail est-elle dans une liste qui a fuité ?
Qu'est-ce qu'un mot de passe fort ?
Comment protéger son mot de passe ?
L'utilité de l'authentification à facteur multiple.
Les enjeux de l'identification numérique appliquée à la santé.

MODULE 4	LES MÉLANGES DES USAGES PERSONNELS ET PROFESSIONNELS & LA MOBILITÉ

Les risques liés à la mobilité.
Les risques du mélange des usages personnels et professionnels.
La recherche d'information via les réseaux sociaux.
Se protéger en situation de mobilité.
Pourquoi ne pas faire confiance aux Wi-Fi publics ?
Bonnes pratiques en télétravail.
VPN, pourquoi tout le monde en parle ?
Quels sont les risques avec votre smartphone et comment le protéger (antivirus, applications de confiance ...) ?

MODULE 5	PHISHING ET SOCIAL ENGINEERING

Qu'est-ce que le social engineering ?
Qu'est-ce que le phishing, le vishing et le smishing ?
Une campagne de phishing réussie, quels impacts ?
Les ransomware diffusé par phishing : mode opératoire et intérêts des cyber-attaquants.
Comment reconnaître un mail suspect ?
Un exemple d'escroquerie bien menée.

MODULE 6	HYGIENE NUMERIQUE AU QUOTIDIEN

L'intérêt des mises à jour.
Utilisation d'outils légitimes.
Bureau « propre » et partage de sessions.
Risques des périphériques USB et gestion de vos périphériques amovibles.
Utilisation d'outils « gratuits » en ligne et risques.
L'utilisation de votre messagerie sécurisée.
Se protéger au quotidien.
Qu'est-ce que le chiffrement et comment cela protège vos données ?
Que faire en cas de compromission d'un poste ?

PRÉREQUIS

Être un professionnel de santé disposant d'un numéro RPPS.
En amont de l'inscription, les prérequis seront vérifiés par e-mail et/ou par téléphone.

ACCESSIBILITÉ

PARTIE E-LEARNING : la formation sera accessible dès réception d'un mail envoyé par nos soins contenant l'accès à la plateforme en ligne.

MODALITÉ ET DÉLAIS D'ACCÈS

Les inscriptions se font depuis le site www.mondcp.fr
Pour les formations en e-learning, les inscriptions sont possibles jusqu'à la veille effective de démarrage de la session, sous réserve du nombre de places disponibles.

MÉTHODES PÉDAGOGIQUES MOBILISÉES

Pour la formation en e-learning, une plateforme digitale sécurisée accessible 24/7.
Fiches de cours téléchargeables à partir de la plateforme e-learning.
Méthodes pédagogiques expositive et active.
Alternance d'apports théoriques et pratiques.
Utilisation de nombreux exercices auto-corrigés et des cas pratiques avec correction.
Contact avec le formateur via un chat, tout au long du parcours.

MODALITÉS D'ÉVALUATION DE LA FORMATION

Evaluations formatives tout au long de la formation.
Evaluation sommative en fin de formation : quizz et auto-évaluation (sur la base d'un questionnaire intial et d'un questionnaire final permettant d'identifier les acquis).
Questionnaire de satisfaction en fin de formation.

VALIDATION DE LA FORMATION

Attestation de réalisation en fin de formation.

ACCESSIBILITÉ AUX PERSONNES EN SITUATION DE HANDICAP

Pour les candidats dont la situation le nécessite, la responsable pédagogique est disponible pour envisager les possibilités d'aménagement de la formation à travers un projet personnalisé de formation.

CONTACT RÉFÉRENTE HANDICAP - Aurélie FANINOZ
04 91 26 27 09 contact@freeforma.fr

FREEFORMA

Organisme de formation pour les professionnels de santé.

Agrément DPC : 9659

04 91 22 51 47
contact@freeforma.fr
Bureau administratif : 375 rue Paradis, 13008 Marseille

SIREN : 849469325
Numéro d'enregistrement DREETS : 93131785413
Ce numéro ne vaut pas agrément.