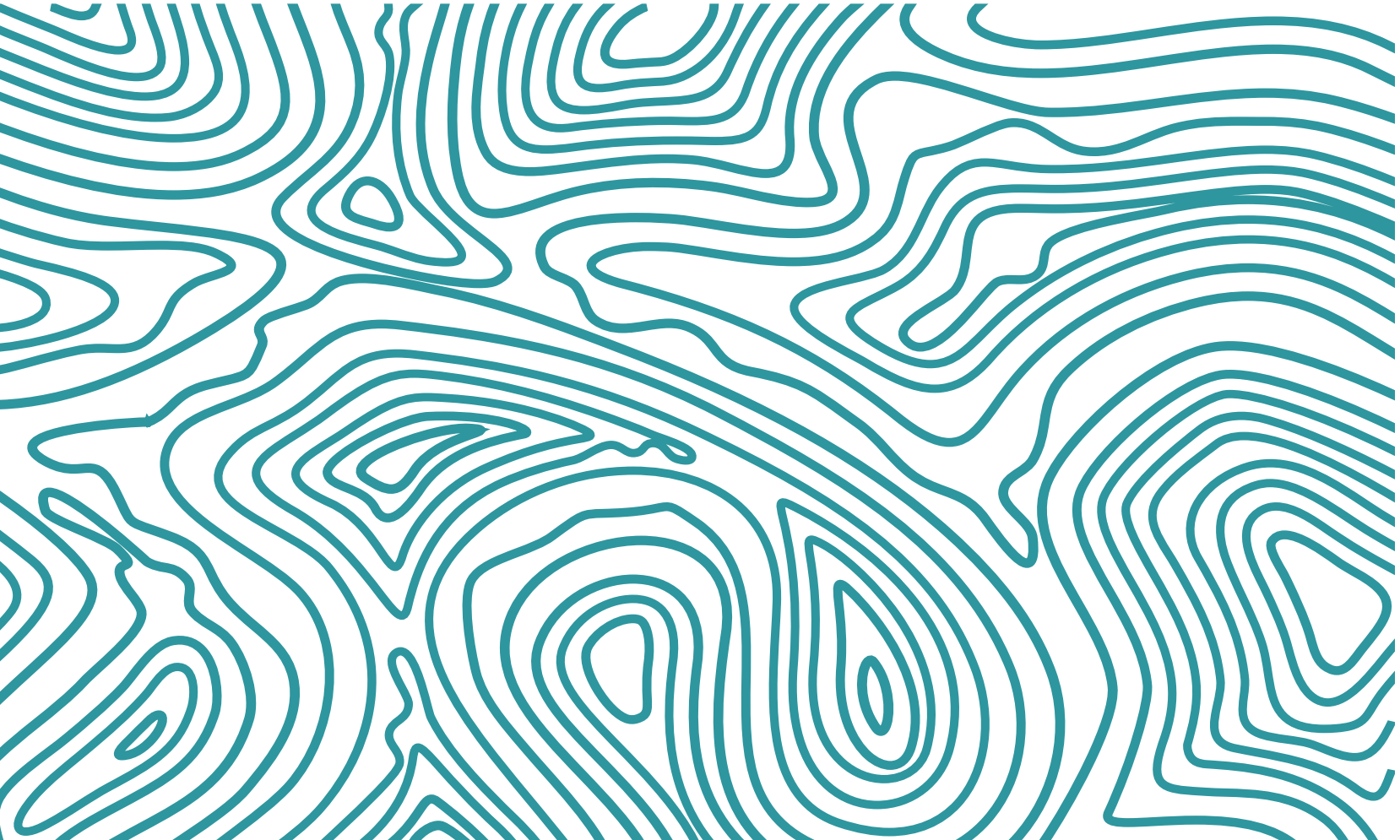
Thématique :

CYBERSÉCURITÉ EN SANTÉ



Médilearn.care

VOTRE FORMATION CONTINUE

MEDILEARN.CARE

medilearn.care

FORMATION CONTINUE | CYBERSÉCURITÉ EN SANTÉ

DESCRIPTION DE LA FORMATION

Officines, hôpitaux, cliniques, laboratoires d'analyse, cabinets médicaux ... 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).

DURÉE : 7h.
La plateforme d'apprentissage est disponible 24h/24 et 7J/7. Vous organisez vos sessions de formation selon vos disponibilités.

PRÉREQUIS
Professions libérales et professionnels salariés. En amont de l'inscription, les prérequis seront vérifiés par e-mail et/ou par téléphone.

INTERVENANT
Formateur qualifié.

PUBLIC CIBLÉ
Pharmaciens titulaires, pharmaciens adjoints, préparateurs en pharmacie, salariés en officine de pharmacie.

E-LEARNING | CODE FORMATION : MP02 **NUMÉRO DPC :** 96592425136 **VOIR LE DESCRIPTIF EN LIGNE**

ÉLÉMENTS DE CONTENU & OBJECTIFS

OBJECTIFS :

Concevoir et maintenir sécurisé son environnement numérique de travail.

Savoir se prémunir et réagir face aux incidents.

Adopter une bonne hygiène numérique.

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

Connaitre 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.

MODULE 1 : 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 2 : 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.
Votre adresse mail est-elle dans une liste qui a fuité ?

ÉLÉMENTS DE CONTENU & OBJECTIFS

MODULE 2 : L'IMPORTANCE DE L'AUTHENTIFICATION - SUITE

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 3 : 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 4 : 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 5 : HYGIÈNE NUMÉRIQUE 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 ?

VOTRE INTERLOCUTEUR DIRECT
04 91 26 27 09
contact@medilearn.care

A votre écoute du lundi au jeudi de 10h à 18h
et le vendredi de 9h à 17h.

TARIF

Voir sur la page descriptive sur notre site internet
OU nous consulter : contact@medilearn.care

CONTACT

SAS EPSA
Médilearn
04 91 26 27 09
contact@medilearn.care
medilearn.care
SIREN : 849469325

ACCÈS AUX PERSONNES EN SITUATION DE HANDICAP

Cette formation peut être adaptée aux personnes en situation de handicap. Pour obtenir des informations, sollicitez notre référent handicap par e-mail : contact@medilearn.care

MODALITÉS D'ÉVALUATION

Evaluation des pratiques professionnelles sur deux tours.

MÉTHODES ET MOYENS PÉDAGOGIQUES

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

MODALITES ET DELAIS D'ACCÈS

Modalités : Les inscriptions sont possibles jusqu'à la veille effective de démarrage de la session, sous réserve du nombre de places disponibles.

Délais d'accès : date selon la disponibilité du formateur.