2024

Approche pratique de la cybersécurité

Side Quest

Une question sur le programme ? Besoin de précisions ? Besoin d'une prise en charge particulière ?
Contactez notre responsable pédagogique : thibault@side-quest.io

Document remis au stagiaire avant son inscription (Article L 6353-8 du Code du Travail)

Les ressources et contenus de la formation sont régulièrement mis à jour. La date du programme correspond également à la date de la dernière mise à jour de la formation. V3 : 04/2024

Approche pratique de la cybersécurité

Objectifs (professionnels)

A l'issue de la formation, le stagiaire sera capable de :

- ✔ Comprendre et savoir reconnaître les principaux types d'attaques
- ✔ Connaître les faits marquants et les statistiques de la cybercriminalité
- ✔ Connaître la menace spécifique qui repose sur l'avocat
- ✔ Savoir quel partenaire contacté en fonction des besoins
- ✔ Elaborer une stratégie basique de cybersécurité
- ✔ Assurer une protection robuste de son cabinet et de son matériel personnel
- ✔ Comprendre la dimension juridique de la protection numérique
- ✔ Contrôler et ajuster son empreinte numérique
- ✔ Avoir une gestion efficace des mots de passe
- ✔ Effectuer des sauvegardes de ses données
- ✔ Utiliser des outils simples de chiffrement
- ✔ Se déplacer hors du cabinet de manière sécurisée
- ✔ Savoir réagir au mieux à une cyberattaque
- ✔ Pouvoir transmettre ce savoir à ses clients et comprendre leurs besoins vitaux en matière de protection

Public

Cette formation est ouverte aux avocats régulièrement inscrits au barreau.

Pré-requis

Être avocat régulièrement inscrit au barreau ou exercer au sein d'un cabinet d'avocat.

Durée

La formation dure 4 heures.

La formation est accessible à tout moment par l'apprenant, une fois régulièrement inscrit. Il peut à tout moment mettre en pause puis reprendre le parcours.

Il dispose d'un an pour terminer la formation à partir de la date d'achat.

Il dispose d'une durée de trois mois pour terminer la formation une fois une fois commencée.

Tarif

Cette formation est dispensée pour un coût de 300€ HT, soit 360€ TTC, hors offre promotionnelle éventuelle.

Modalités et délais d'accès

L'inscription est réputée acquise lorsque l'apprenant a payé l'intégralité de la formation et a signé la convention de formation.

Moyens pédagogiques, techniques et d'encadrement

Méthodes et outils pédagogiques

Méthodes pédagogiques : Magistrale, Démonstrative et active.

Outils pédagogiques : Vidéos, animations, screencast, QCM

Supports pédagogiques : A la fin de la formation, l'apprenant reçoit un document au format PDF reprenant les savoirs essentiels de la formation.

Prise en compte du handicap : 100% en ligne avec rythme modulable, scriptes à disposition des apprenants si nécessaire, aménagements supplémentaires possibles sur demande avec étude au cas par cas.

Contacter le référent handicap : thibault@side-quest.io

Eléments matériels de la formation

Supports techniques : formation 100% en ligne via la plateforme Side quest formation, créée avec Learnybox.

Équipements devant être amenés par l'apprenant : l'apprenant doit avoir un ordinateur, tablette ou smartphone ainsi qu'une connexion internet pour accéder au portail de la formation.

Documentation : Liste de ressources complémentaires délivrées au cours de la formation, support pédagogique livré en fin de formation.

Compétences des formateurs

La formation sera assurée par Thibault OUDOTTE : co-fondateur de Side quest et juriste en cybersécurité

Formation ouverte ou à distance FOAD

Cette formation est exclusivement prodiguée à distance.

Le stagiaire doit suivre l'ensemble des vidéos en intégralité pour valider la formation, il doit également répondre aux questions intermédiaires (entre les modules) ainsi qu'aux questions en fin de partie.

Des ressources complémentaires sont mises à disposition de l'apprenant, il n'est pas obligatoire de les consulter pour valider la formation.

La formation est réalisée via la plateforme Side quest, l'apprenant peut à tout moment solliciter l'équipe pédagogique de Side quest pour une assistance technique (dans les limites de nos capacités en ce qui concerne la plateforme) ou pédagogique ou pour toute autre question liée au contenu de la formation (Responsable pédagogique : Thibault Oudotte).

L'apprenant peut nous contacter par email (contact@side-quet.io), par téléphone (07 66 49 18 76), via notre site internet (side-quest.io) ou encore via les réseaux sociaux.

Le délai habituel de réponse est de 48h.

side quest

Contenu (🔲 = Quiz)

Présentation de la plateforme

Introduction générale

Partie 1 : Etat des lieux de la menace cyber

- *Profils d'attaquants et d'attaques*
- *Les rançongiciels*
- *Le hameçonnage*
- *Personne du milieu et WiFi public*
- *Keylogger et espionnage*
- *Attaque en déni de service*
- *Le vol et les fuites de données*
- *La menace et l'avocat*
- *Les impacts d'une cyberattaque*
- *Quiz* 🔲

Partie 2 : Les grands acteurs à connaître

- *L'ANSSI*
- *La CNIL et le RGPD*
- *Cybermalveillance.gouv.fr*

Partie 3 : Stratégie de cybersécurité

- *Cartographier ses données*
- *Le budget de la cybersécurité*
- L'assurance du risque cyber
- *Formaliser les process et s'entraîner*
- *Quiz* 🔲

Partie 4 : Les mesures juridiques

- *La charte informatique*
- *Contrats de sous-traitance*

side quest

Partie 5 : Contrôler son empreinte numérique

- *Ce que révèlent vos données*
- *Focus réseaux sociaux*

Partie 6 : Les bonnes pratiques au quotidien

- *Séparer usage pro et usage perso*
- *Bien choisir et bien gérer son matériel*
- *Bien choisir ses mots de passe*
- *Retenir ses mots de passe : utiliser un coffre-fort*
- *Effectuer des sauvegardes régulières*
- *Quiz* ❓

Partie 7 : Les bonnes pratiques en déplacement

- *Partir avec son ordinateur*
- *Se connecter dans les lieux publics : le fonctionnement du VPN*
- *La protection du téléphone portable*

Partie 8 : Bien configurer son matériel

- Activer ses pare feux et utiliser un antivirus
- *Protéger sa session par mot de passe*
- *Gérer les droits des utilisateurs*
- *Toujours procéder aux mises à jour*
- *Les solutions de chiffrement*
- *Protéger sa boite mail*
- *Naviguer en toute sécurité*
- *La sécurité et les objets connectés*
- *Quiz* ❓

Partie 9 : Réagir à une cyberattaque

- *Les réflexes à avoir en cas de cyberattaque*
- *Gestion de crise et communication*
- *Porter plainte*
- *Quiz* ❓

Conclusion

Suivi et évaluation

Exécution de l'action

Les moyens permettant de suivre l'exécution de l'action sont inclus dans la plateforme, ils permettent d'attester le suivi du parcours par l'apprenant ainsi que sa participation aux quiz et exercices.

Modalités d'évaluation des résultats (ou d'acquisition des compétences)

Pour déterminer si l'apprenant a acquis les connaissances fixées dans les objectifs, on se base sur des QCM et des exercices d'application en ligne, avec correction automatique.