Formation Comment se protéger de la cybercriminalité

Comment se protéger de la Cybercriminalité

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La cybercriminalité est une menace qui touche toutes les organisations, sociétés, administrations. Elle a explosé de 60% entre 2019 et 2020. La question qui importe est de savoir si votre organisation sera prête lorsqu'elle se fera attaquer.

Référence	MAG95
Durée	2 jours (14h)
Tarif	1 990 €HT

Objectifs

| Identifier les enjeux de la cybercriminalité
| Être capable d'identifier les biens essentiels à protéger
| Pouvoir identifier les sources de risques dans son organisation
| Identifier comment détecter des actes de malveillance
| Savoir réagir face à un acte de malveillance

Public

| RSSI, Fonction SSI, direction générale, DSI, juristes

Prérequis

| Aucun

Programme de la formation

L'évolution de la cybercriminalité
| Internet aujourd'hui, données et chiffres
| Les nouveaux marchés de la cybercriminalité
| Approche économique de la cybercriminalité
| Comprendre le darknet
| Les outils des cybercriminels (botnets, attaques etc...)
| Quelques typologies d'attaque

Droit des TIC et organisation de la cybersécurité en France
| Organisation de la cybersécurité en France
| Contexte juridique
| Droit des TIC
| La lutte contre la cybercriminalité, ANSSI et cybermalveillance
| Le rôle de la CNIL et la protection des données personnelles

Protéger son organisation
| Lexique et définitions (vulnérabilités, menaces, risques...)
| Les enjeux des Systèmes d'Information
| Identifier les biens essentiels et les biens supports
| Intégrer la sécurité au sein de son organisation
| Intégrer la sécurité au sein d'un projet
| Identification des difficultés liées à la prise en compte de la sécurité

Identifier et prévenir les sources de risques
| Gouvernance et cybersécurité, définition des rôles et responsabilités
| Définir une stratégie de sécurité des systèmes d'information
| La Charte Informatique
| La gestion des contrats

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 25 au 26 juin 2024
du 29 au 30 août 2024
du 8 au 9 octobre 2024
du 21 au 22 novembre 2024
du 19 au 20 décembre 2024

PARIS

du 18 au 19 juin 2024
du 29 au 30 août 2024
du 1er au 2 octobre 2024
du 21 au 22 novembre 2024
du 12 au 13 décembre 2024

VOIR TOUTES LES DATES

| Mettre en place un système de gestion des risques
| Aperçu des ISO 27001 et 27005

Prévenir les risques : les bonnes pratiques
| Les contrôles d'accès (physiques, logiques...)
| La gestion des comptes administrateurs
| La gestion des mots de passe
| Gérer les développements, les mises à jours et les déploiements
| Mettre en place une procédure d'escalade d'incidents
| Procédures ANSSI et CNIL de déclaration d'actes de malveillance

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.