Formation Sensibilisation à la cybersécurité

Sécurité des SI, des données personnelles et continuité d'activité

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

L'utilisation des ressources du système d'information n'est pas sans risque. Cette sensibilisation présente à l'aide de très nombreux exemples les bonnes pratiques de l'utilisateur sédentaire, nomade ou en télétravail pour limiter les risques d'erreur ou de malveillance.

Référence	RES104
Durée	1 jour (7h)
Tarif	915 €HT

Objectifs

| Utiliser les bonnes pratiques pour limiter les risques juridiques et opérationnels
| Protéger les informations en adéquation avec les besoins métiers

Public

| Tous les salariés d'une entreprise

Prérequis

| Aucun

Programme de la formation

Introduction
| Les préjugés à surmonter
| Les valeurs essentielles à protéger
| Les périmètres
| Les menaces

L'organisation et les responsabilités
| La direction générale
| Les directions métiers
| La DSI
| Les sous-traitants
| La voie fonctionnelle SSI et le RSSI
| La voie fonctionnelle protection de la vie privée et le DPO
| Les administrateurs techniques et fonctionnels
| Les utilisateurs

Les référentiels SSI et vie privée
| Les politiques
| Les chartes
| Les guides et manuels
| Les procédures

Vision synthétique des obligations légales
| Disciplinaire
| Contractuelle
| Civiles
| Pénales
| Le cas du contrôle par l'employeur : utilisation professionnelle et non-professionnelle

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
le 14 juin 2024
le 27 juin 2024
le 13 septembre 2024
le 10 octobre 2024

PARIS
le 14 juin 2024
le 20 juin 2024
le 13 septembre 2024
le 3 octobre 2024

LILLE
le 14 juin 2024
le 15 novembre 2024

LYON
le 14 juin 2024
le 15 novembre 2024

VOIR TOUTES LES DATES

Les menaces
| La divulgation d'information spontanée
| L'ingénierie sociale et l'incitation à dire ou faire
| Le lien avec l'intelligence économique
| Le lien avec l'espionnage industriel

Les risques
| Vol, destruction
| Virus
| Les aspirateurs à données
| Le phishing /l'hameçonnage
| Les malwares
| Les spywares
| L'usurpation
| L'usurpation
| Les virus
| Le cas des réseaux sociaux

Les bonnes pratiques d'évaluation de la sensibilité de l'information
| La classification par les impacts, (juridiques, opérationnels, financiers, image, sociaux)
| L'échelle d'impact
| Les pièges

Les bonnes pratiques pour les comportements généraux
| A l'intérieur des établissements
| A l'extérieur des établissements

Les bonnes pratiques d'utilisation des supports d'information sensible pour les phases de conception, stockage, échanges et fin de vie
| Papier
| Environnement partagé
| Environnement individuel sédentaire
| Environnement individuel mobile

Les bonnes pratiques d'utilisation des ressources du système d'information
| Installation et maintenance : postes fixes, équipements nomades, portables, ordiphones
| Identification et authentification
| Échanges et communications : intranet, internet, contrôle des certificats serveurs, les échanges de fichiers via la plate-forme institutionnelle, le nomadisme, les télétravailleurs et le VPN de télé accès, email, la consultation en Web mail, signature, chiffrement, Cloud, réseaux sociaux et forums thématiques professionnels et privés, téléphonie
| Stockages et sauvegardes (clés usb, locales, serveurs, ...)
| Archivages
| Anonymisation
| Destruction ou recyclage

Conclusion
| Les engagements de responsabilité

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.