



SEMINAIRE DE FORMATION SENSIBILISATION A LA SECURITE INFORMATIQUE

CONTACTEZ-NOUS
Tél 01 44 69 33 49

Un Centre de Formation orienté Nouvelles Technologies
Une équipe disponible et réactive à votre écoute
Cours sur mesure adaptés à votre activité
Des formateurs hautement qualifiés



La Sécurité de votre Système d'Information peut être mise en défaut par l'attitude de vos collaborateurs, face à des situations critiques, ce qui vous fait prendre des risques majeurs.

La Sécurité du Système d'Information est un vaste sujet, bien souvent mal abordé, car traité essentiellement au travers de **réponses techniques**, en **négligeant le caractère humain** et donc les problématiques internes.

La meilleure protection est la PREVENTION !

Il est vital pour votre Entreprise de faire former votre personnel, afin d'**anticiper** et donc d'**éviter** des risques inconsidérés qui mettront tôt ou tard votre Entreprise en danger : perte ou vol de données, perte d'exploitation, coûts de remise en état, perte de clients, ...

OBJECTIFS

- **Sensibiliser votre personnel** afin de tendre vers le **risque ZERO**,
- **Adopter les bonnes attitudes et réflexes** face aux différents mécanismes et techniques qui peuvent mettre en défaut la sécurité de votre Système d'Information,
- **Optimiser la disponibilité de votre S.I.** en évitant la malveillance ou l'usage abusif, ce qui aura des répercussions positives sur votre activité et votre productivité.

Public : Utilisateurs de systèmes informatiques, désirant mieux se protéger et contribuer à l'intégrité de leur Système d'Information.

Pré-requis : Utilisateurs de services de Systèmes d'Informations.

Durée de la formation : 3 jours

Horaire : de 09h00 à 17h00

Coût de la formation :

- Inter-entreprises :** 1 490 € HT stagiaire
- Intra-entreprise :** la formation peut se dérouler dans votre établissement, avec un maximum de 8 stagiaires/session

PROGRAMME DE FORMATION SENSIBILISATION A LA SECURITE INFORMATIQUE

Module 1 : **La sécurité informatique : définitions, rappels**
 S.I.
 S.S.I.
 Management du S.I.
 La sécurité est l'affaire de tous
 Qualifier les risques et identifier les zones sensibles

Module 2 : **Historique : piratage, techniques de contamination et d'attaques**
 Piratage
 Virus
 Spams
 Vers
 Phishing
 Pharming
 Hackers



- Module 3 : **Le contexte : constat, sécurité mise à l'épreuve quotidiennement, répercussions sur l'activité, la productivité, responsabilité juridique**
Contexte économique des Directions Informatiques
Sécurité mise à l'épreuve de l'extérieur
Sécurité mise à l'épreuve de l'intérieur
Répercussions sur la productivité
Répercussions sur l'activité de l'entreprise et ses clients
Répercussions juridiques sur les dirigeants
- Module 4 : **Les coûts de la Sécurité Informatique**
Coûts organisationnels
Coûts humains
Coûts technologiques
Coûts ponctuels
- Module 5 : **Les coûts et les dégâts d'une Sécurité inadaptée**
Coûts récurrents
Coûts occasionnels
Coûts suite à sinistres
- Module 6 : **Les risques : contamination, attaques, malveillances, vol d'information**
Virus, Vers, Chevaux de Troie, ...
Spywares, Adwares
Phishing, Pharming
Consultation de sites à risque ou indésirables
Téléchargements
Radio / vidéo en ligne
Supports amovibles
Sinistres, malveillances
Espionnage, vol d'informations
Piratage
- Module 7 : **Les enjeux sécuritaires, financiers, légaux**
Enjeux sécuritaires
Enjeux financiers
Enjeux légaux
- Module 8 : **Les attaques et contaminations : techniques, parades, attitudes à adopter**
Le hacking
Motivations
Processus des attaques
Familles d'attaques
Contamination Web sur Internet
- Module 9 : **L'ingénierie sociale, attitudes à adopter : technique redoutable contre laquelle la sécurité matérielle sera systématiquement mise en défaut**
Définition
Les risques
Usurpation d'identité
PSI et l'ingénierie sociale
Attitudes à adopter
- Module 10 : **Analyse des risques, méthodes d'évaluation**
Evaluation des risques
Méthodes d'évaluation
Les solutions
- Module 11 : **Conclusions, conseils, préconisations**
Conseils
Préconisations
- Module 12 : **Questions-réponses : débat ouvert**

« [Inscriptions sur notre site web](#) »

Suivi personnalisé :

Raphaël REINA Tél. 06.69.06.42.27

rreina@academie-unix.com