

CYBERSECURITE SENSIBILISATION DES UTILISATEURS

Public	Tous les utilisateurs ayant accès au Système d'Information via un poste informatique.
Durée	1 journée - 7 heures
Pré-requis	Aucune connaissance particulière.
Objectifs	Comprendre la typologie de risques liés à la sécurité SI et les conséquences possibles Identifier les mesures de protection de l'information et de sécurisation de son poste de travail Favoriser la conduite de la politique de sécurité SI de l'entreprise
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

LA SÉCURITÉ INFORMATIQUE : COMPRENDRE LES MENACES ET LES RISQUES

- Introduction : cadre général, qu'entend-on par sécurité informatique (menaces, risques, protection) ?
- Comment une négligence peut-elle créer une catastrophe ? Quelques exemples. La responsabilité.
- Les composantes d'un SI et leurs vulnérabilités. Systèmes d'exploitation client et serveur.
- Réseaux d'entreprise (locaux, site à site, accès par Internet).
- Réseaux sans fil et mobilité. Les applications à risques : Web, messagerie...
- Base de données et système de fichiers. Menaces et risques.
- Sociologie des pirates. Réseaux souterrains. Motivations.
- Typologie des risques. La cybercriminalité en France. Vocabulaire (sniffing, spoofing, smurfing, hijacking...).

LA PROTECTION DE L'INFORMATION ET LA SÉCURITÉ DU POSTE DE TRAVAIL

- Vocabulaire. Confidentialité, signature et intégrité. Comprendre les contraintes liées au chiffrement.
- Schéma général des éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Quelle menace sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ? Le port USB. Le rôle du firewall client.

L'AUTHENTIFICATION DE L'UTILISATEUR ET LES ACCÈS DEPUIS L'EXTÉRIEUR

- Contrôles d'accès : authentification et autorisation.
- Pourquoi l'authentification est-elle primordiale ?
- Le mot de passe traditionnel.
- Authentification par certificats et token.
- Accès distant via Internet. Comprendre les VPN.
- De l'intérêt de l'authentification renforcée.

COMMENT S'IMPLIQUER DANS LA SÉCURITÉ DU SI ?

- Analyse des risques, des vulnérabilités et des menaces.
- Les contraintes réglementaires et juridiques.
- Pourquoi mon organisme doit respecter ces exigences de sécurité ?
- Les hommes clés de la sécurité : comprendre le rôle du RSSI et du Risk manager.
- Agir pour une meilleure sécurité : les aspects sociaux et juridiques. La CNIL, la législation.
- La cybersurveillance et la protection de la vie privée.
- La charte d'utilisation des ressources informatiques.
- La sécurité au quotidien. Les bons réflexes. Conclusion

NOUS CONTACTER

Siège social

16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone

04 76 23 20 50 - 06 81 73 19 35

Centre de formation

87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

E-mail

contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !



ACF Audit Conseil Formation



@ACF_Formation



ACFauditconseilformation