SARL ONEO
1025 rue Henri Becquerel
Parc Club du Millénaire, Bât. 27
34000 MONTPELLIER
N° organisme : 91 34 0570434

Nous contacter :
04 67 13 45 45
www.ait.fr
contact@ait.fr

Référence	**4-SE-WIND**
Durée	**1 jour (7 heures)**
Éligible CPF	**NON**
Mise à jour	**07/01/2025**

Former et sensibiliser les utilisateurs à la sécurité informatique

Objectifs pedagogiques

- Etre sensibilisé aux menaces informatiques auxquelles les collaborateurs peuvent être directement confrontés dans leur activité professionnelle et privée, pour mieux les former et les informer au quotidien
- Comprendre les problématiques liées à la sécurité informatique
- Comprendre en quoi la prévention est nécessaire
- Adopter les bonnes attitudes et réflexes
- Savoir mettre en œuvre les solutions concrètes proposées

Public concerne

Toute personne concernée par une démarche sécurité au sein de l'entreprise

Prerequis

Pas de prérequis spécifiques

Moyens pedagogiques

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Remise d'un support de cours.

Modalites d'evaluation

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Attestation de stage à chaque apprenant,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

Moyens techniques en presentiel

Accueil des stagiaires dans une salle dédiée à la formation équipée à minima d'un vidéo projecteur et d'un tableau blanc et/ou paperboard.

Pour les formations nécessitant un ordinateur, un PC est mis à disposition de chaque participant.

Moyens techniques en distanciel

A l'aide d'un logiciel (Teams, Zoom…), d'un micro et éventuellement d'une caméra les apprenants interagissent et communiquent entre eux et avec le formateur.

Sessions organisées en inter comme en intra entreprise.

L'accès à l'environnement d'apprentissage ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.

Pour toute question avant et pendant le parcours, assistance technique à disposition au 04 67 13 45 45.

Organisation

Délai d'accès : 5 jours ouvrés
(délai variable en fonction du financeur)

Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

Accessibilite

Les personnes en situation d'handicap sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

Pour tout renseignement, notre référent handicap reste à votre disposition : mteyssedou@ait.fr

Profil formateur

Nos formateur sont des experts dans leurs domaines d'intervention

Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

Certification possible

TOSA

Former et sensibiliser les utilisateurs à la sécurité informatique

LA SECURITE ET L'ENTREPRISE

- ☐ Quelques exemples concrets de piratage
- ☐ Facteurs techniques : système, logiciel, réseau, web, données
- ☐ Facteur humain
- ☐ Identifier la valeur : Ce qu'il n'est pas « grave » de perdre, quels sont les biens à protéger ?
- ☐ Les moyens pour garantir une meilleure sécurité
- ☐ A quoi sert une charte d'utilisation des ressources informatiques ?

LOI ET SECURITE INFORMATIQUE

- ☐ Le cadre législatif de la sécurité
- ☐ Les responsabilités civiles et pénales
- ☐ Le rôle de la CNIL et son impact pour la sécurité en entreprise
- ☐ Le règlement intérieur.
- ☐ Synthèse : charte morale, interne/loi

LES MOTS DE PASSE

- ☐ Ce que l'on peut faire avec le mot de passe d'autrui
- ☐ Qu'est-ce qu'une attaque par dictionnaire ?
- ☐ Pourquoi peut-on être forcé de respecter une stratégie de nomenclature ?
- ☐ Ne pas confondre la base de compte locale et celle du serveur
- ☐ Les devoirs et comportements à adopter vis-à-vis des tiers.
- ☐ Les comportements à l'intérieur de l'entreprise.
- ☐ Les comportements à l'extérieur de l'entreprise.

LES PERIPHERIQUES ET LE POSTE DE TRAVAIL

- ☐ Les risques encourus avec les périphériques USB, CD, DVD
- ☐ Le poste de travail pour Windows (C :, D :, E :, …)
- ☐ Disque interne/externe, clé USB, réseau : quelles différences pour les risques ?
- ☐ Exemple de propagation de virus par clef USB
- ☐ Les réflexes à adopter avec les « corps étranger »

COMPRENDRE LES BASES DU RESEAU

- ☐ (20 minutes seulement sur ce module)
- ☐ Chaque équipement (PC, Serveur, …) dispose d'une adresse IP
- ☐ Vocabulaire réseau de base (passerelle, DNS, DHCP)
- ☐ Chaque application est référencée par un numéro (port)
- ☐ Que fait un firewall d'entreprise ?
- ☐ Et ce qu'il ne fait pas à la place des utilisateurs …
- ☐ Risques liés à l'accueil du portable d'un visiteur dans l'entreprise
- ☐ Intérêts d'utiliser un serveur Proxy en entreprise pour accéder au Web

COMPORTEMENT PAR RAPPORT A LA MESSAGERIE

- ☐ Le mail un simple fichier texte ?
- ☐ La réception des messages (SPAM, faux messages…)
- ☐ Le mauvais usage de la retransmission des messages
- ☐ Les courriers électroniques de taille importante
- ☐ L'usurpation d'identité

RISQUES LIES A INTERNET

- ☐ Navigation et surprises !
- ☐ Les problèmes liés au téléchargement de fichiers
- ☐ Limites de l'ultra protection des navigateurs
- ☐ Peut-on « rattraper » une information divulguée ?
- ☐ La téléphonie utilise maintenant les réseaux de données

SYNTHESE ET CONCLUSION

- ☐ Synthèse des points abordés
- ☐ Savoir évaluer les risques

REGLES DE BONNES CONDUITES