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-CYBER**
Durée	**1 jour (7 heures)**
Éligible CPF	**NON**
Mise à jour	**04/03/2026**

Cybersécurité: utiliser l'informatique en toute sécurité

Objectifs pedagogiques

- Etre sensibilisé aux menaces informatiques auxquelles nous pouvons être confrontés dans notre activité professionnelle et privée
- Adopter les bonnes attitudes et réflexes
- Devenir un cybercitoyen pour diffuser les bonnes pratiques autour de soi

Public concerne

Tout utilisateur d'outils informatiques, ordinateurs, tablettes, smartphones

Prerequis

Utilisation de l'informatique

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 Cybercitizen
Certificateur ISOGRAD

Cybersécurité: utiliser l'informatique en toute sécurité

LA SECURITE, LA LOI, L'UTILISATEUR ET L'ENTREPRISE

- ☐ Quelques exemples concrets de piratage
- ☐ Facteurs techniques : système, logiciel, réseau, web, données
- ☐ Facteur humain
- ☐ A quoi sert une charte d'utilisation des ressources informatiques ?
- ☐ Le cadre législatif de la sécurité
- ☐ Les responsabilités civiles et pénales
- ☐ 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 »

LE VOCABULAIRE DE LA PROTECTION EN ENTREPRISE… ET A LA MAISON

- ☐ Définition, rôle : Pare-feu, VPN, proxy, box internet…

COMPORTEMENT PAR RAPPORT A LA MESSAGERIE

- ☐ Le mail, un simple fichier texte ?
- ☐ La réception des messages (SPAM, faux messages…)
- ☐ Ne pas devenir un spammeur : dangers de l'envoi en nombre
- ☐ 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
- ☐ Règles de bonnes conduites

POINTS FORTS DE LA FORMATION

- ☐ Nombreux exemples dans la vie professionnelle et dans la vie privée
- ☐ Quiz de début de séquence, quiz de fin de séquence
- ☐ Support de cours détaillé
- ☐ Fiches de synthèses des bonnes conduites
- ☐ Adapatation possible à la charte informatique de l'entreprise