

SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

Durée & Format

Durée : 7 heures

Format disponible : Présentiel ou Distanciel

Tarifs

Tarif public intra : Consulter notre [site Internet](#)

Tarif public inter : Consulter notre [site Internet](#)

Public visé

- Toute personne souhaitant se familiariser avec les différents concepts liés à la sécurité des Technologies de l'information

Prérequis

- Avoir une utilisation basique de son ordinateur PC ou Mac

Objectifs pédagogiques

À l'issue de cette formation, l'apprenant sera capable de :

- Maîtriser les concepts clés relatifs à l'importance d'assurer la sécurité des informations et des données, d'assurer leur sécurité physique, d'éviter le vol de données personnelles et de protéger leur vie privée.
- Protéger un ordinateur, un dispositif numérique mobile, un réseau contre les logiciels malveillants (malware) et les accès non autorisés.
- Maîtriser les différents types de réseaux, de connexions et les composants spécifiques tels que le pare-feu (firewall) qui peuvent poser problème lors des connexions.
- Naviguer sur le World Wide Web et communiquer en toute sécurité sur Internet.
- Maîtriser les problèmes de sécurité liés à la communication, notamment en matière de courrier électronique et de messagerie instantanée (MI – IM/Instant messaging).
- Sauvegarder et restaurer des données de manière appropriée et sécurisée, entreposer ses données et ses dispositifs numériques mobiles en toute sécurité.

Programme et déroulement

Jour 1 – Matin

Maîtriser les concepts de sécurité

- Quelles menaces sur les données ?
- Quelle est la valeur de l'information ?
- Sécurité des données personnelle : Protéger la vie privée
- Le RGPD : Règlement général sur la protection des données
- La sécurité physique des fichiers
- Éviter le vol de données personnelles

Se protéger des logiciels malveillants

- Définitions des différents logiciels malveillants et fonctionnement
- Les différents types de menaces
- Quels outils pour se protéger ?



Assurer la sécurité de ses réseaux

- Qu'est-ce qu'un réseau ?
- Quels types de réseaux ?
- Se connecter aux réseaux
- Sécuriser son environnement sans fil
- Quelques règles de contrôle d'accès
- Le Fire-Wall

Jour 1 – Après-midi

Naviguer sur le Web en toute sécurité

- La Navigation Web laisse des traces : lesquelles ?
- Points à vérifier avant d'envoyer des informations sur un site
- Savoir gérer les cookies
- Navigation privée
- Risques des réseaux sociaux
- Exercer son droit à l'oubli

Sécuriser ses communications

- Envoi d'emails
- Les pièces jointes
- Quelles menaces sur la messagerie ?
- Fonctionnement et risques liés Messagerie instantanée (MI/IM)

Gérer de la sécurité des données

- Sécuriser et sauvegarder les données
- Restaurer des données
- Destruction sécurisée
- Stocker des données en ligne

Questions/Réponses

Certification

Consulter le programme sur notre [site internet](#) pour identifier si cette formation est certifiante.

Modalités pédagogiques

- Explications théoriques suivies de pratiques guidées puis de mises en autonomie.
- Exercices autonomes et réguliers pour assurer l'assimilation

Moyens et supports pédagogiques

Votre formation a lieu en présentiel :

- 1 vidéoprojecteur par salle
- 1 ordinateur

Votre formation se déroule à distance avec :

- 1 ordinateur
- 1 connexion Internet
- 1 adresse e-mail valide
- 1 équipement audio (micro et enceintes ou casque)
- 1 Webcam (facultatif – dans l'idéal)
- 1 deuxième écran (facultatif – dans l'idéal)

Votre formation se déroule sur notre plate-forme de formation avec :

- 1 ordinateur
- 1 connexion Internet
- 1 adresse e-mail valide
- 1 équipement audio (micro et enceintes ou casque - facultatif)

Support stagiaire :

À l'issue de la formation, les exercices et travaux pratiques réalisés, leurs corrigés ainsi qu'un support de cours dématérialisé sera fourni à chaque stagiaire par e-mail ou via la plate-forme FOAD.

Evaluation et suivi

Les objectifs pédagogiques sont évalués et suivis grâce à différentes **méthodes adaptées aux acquisitions de compétences visées**. Nos formateurs réalisent ces évaluations **tout au long de la formation**, que ce soit pendant les séances synchrones ou asynchrones. Voici une liste non exhaustive des méthodes d'évaluation pouvant être utilisées en formation :

- **Questionnaire** de vérification de connaissances (Quiz)
- Réalisation de **Travaux Pratiques** : production ou amélioration d'un fichier
- **Mises en situation** et grilles d'analyse
- **Serious Game** : jeu de rôles et analyse
- **Activités interactives** à travers l'utilisation d'une plate-forme connectée
- ...

Toutes nos formations intègrent **une auto-évaluation** via notre Extranet Stagiaire au début et à la fin de chaque action de formation. Cet outil offre à chacun la possibilité de mesurer sa progression par rapport aux objectifs pédagogiques visés et leurs atteintes.

Profil formateur

Nos formateurs sont certifiés à l'issue d'un parcours organisé par nos soins. Ils bénéficient d'un suivi de maintien et d'évolution de leurs compétences aussi bien au niveau technique que pédagogique. Chacun de nos formateurs a bénéficié d'une formation spécifique à l'animation de classe virtuelle et à l'utilisation des solutions de formation à distance du Groupe ARKESYS.

Support stagiaire

À l'issue de la formation, les exercices et travaux pratiques réalisés, leurs corrigés ainsi qu'un support de cours dématérialisé sera fourni à chaque stagiaire via son extranet stagiaire.

Accessible à tous

ARKESYS.NET

70 rue Bergson – 42000 Saint-Étienne
04 28 95 15 82 - info@arkesys.fr
SAS AU CAPITAL DE 60 000 € - SIRET : 501 033 609 00030
ETS secondaire : 58 avenue Debourg - 69007 Lyon - SIRET : 501 033 609 00048
ETS secondaire : 293 route de la Seyne - 83190 Ollioules - SIRET : 501 033 609 00055

Cette formation est accessible à toute personne en situation de handicap. Notre référent handicap prendra contact avec les stagiaires concernés pour adapter l'animation à leurs besoins et rendre l'apprentissage accessible à tous. Enfin, nos centres de formation sont accessibles aux personnes à mobilité réduite. [En savoir plus](#)