Best-of Certifiante

Ref. SEC-POST

Sensibilisation à la sécurité du poste de travail

1 jour (7 heures) | Perfectionnement | Présentiel ou classe à distance

à partir de
645 € HT par personne (TVA en vigueur)

Repas inclus en présentiel

Contenu mis à jour le 30/09/2026. Document téléchargé le 06/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Définir les principaux enjeux de la cybersécurité
- Identifier les menaces courantes (phishing, ransomware, malware, ingénierie sociale…)
- Adopter les bonnes pratiques de sécurité numérique au quotidien
- Sécuriser les équipements, l'accès et les données
- Utiliser Internet, la messagerie et les outils collaboratifs de manière sécurisée
- Réagir efficacement face à un incident de sécurité.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

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

Prérequis

Savoir utiliser un ordinateur sous Windows ou macOS et avoir une bonne culture informatique.

Programme

1 Pendant votre formation

Sensibilisation à la sécurité du poste de travail

Jour 1 - Matin

Introduction à la cybersécurité et valeur de la donnée

- Définir le vocabulaire cyber et les concepts clés
- Comprendre les impacts des cyberattaques sur les organisations
- Appréhender les enjeux de la cybersécurité et la responsabilité de l'utilisateur
- Identifier les données personnelles et sensibles (notions de base du RGPD)
- Comprendre les principes de confidentialité, d'intégrité et de cycle de vie de la donnée

Les menaces et attaques informatiques

- Identifier le panorama des cybermenaces
- Reconnaître les techniques de phishing, spear phishing et d'ingénierie sociale
- Identifier les différents logiciels malveillants (malware, virus, trojans, spyware)
- Comprendre le fonctionnement d'un ransomware et les attaques par mot de passe
- Repérer les faux sites web et les arnaques numériques

Sécurité des postes de travail et protection locale

- Comprendre l'importance de la mise à jour des systèmes
- Utiliser un antivirus, un antimalware et un pare-feu
- Appliquer le chiffrement des données
- Sécuriser l'usage des périphériques (clés USB)
- Gérer la sécurité des équipements personnels (BYOD) dans un cadre professionnel

Exemples de travaux pratiques (à titre indicatif)

- *Analyser le contenu d'une clé USB avec un antivirus*
- *Crypter des données sensibles ou des dossiers*
- *Réaliser des exercices de détection d'arnaques et d'ingénierie sociale*

Jour 1 - Après-midi

Sécurité sur les réseaux et télétravail

- Comprendre l'utilité d'un VPN et des accès distants sécurisés
- Etre conscient des risques liés au Wi-Fi public
- Assurer la sécurité globale en situation de télétravail
- Protéger les visioconférences et sécuriser les accès distants

Contrôle d'accès et identités

- Appliquer une politique de mots de passe robuste
- Utiliser des gestionnaires de mots de passe
- Comprendre et mettre en place l'authentification multi-facteur (MFA)
- Identifier les risques liés au partage des accès et au Shadow IT

Navigation Internet, messagerie et outils collaboratifs

- Choisir les réglages appropriés pour sécuriser son navigateur web
- Identifier le protocole HTTPS, les certificats et effectuer des téléchargements sécurisés
- Utiliser les emails de manière sécurisée (pièces jointes, liens malveillants)
- Identifier les outils collaboratifs, les réseaux sociaux et les risques associés
- Assurer le partage sécurisé des documents en équipe

Sauvegarde et gestion des incidents

- Mettre en place des sauvegardes de données et savoir les restaurer
- Appliquer les procédures d'alerte et détecter les incidents
- Isoler un poste compromis et réagir face à une attaque (ex : ransomware)
- Adopter les réflexes cyber au quotidien et identifier les ressources de veille (ex : cybermalveillance.gouv.fr)

Exemples de travaux pratiques (à titre indicatif)

- *Mettre en place un MFA avec Authenticator*
- *Retrouver sur cybermalveillance.gouv.fr la nature et le risque associé à une attaque*

Certification (en option)

- Prévoir l'achat de la certification en supplément
- L'examen (en français) sera passé soit à la fin de la formation, soit ultérieurement dans nos centres de formation
- Celui-ci se compose de 36 questions (QCM et questions à zones sensibles, en ligne) pour une durée moyenne de 35 minutes (75% de bonnes réponses sont nécessaires pour valider l'examen lié au module)

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.
Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Accessibilité aux personnes en situation de handicap

Détails de la session

Le 18 novembre 2026 (1 jour / 7 heures)

Lyon

Le 18 novembre 2026 Lyon

- 18 novembre 2026 ---------- 9h00 - 17h00