NOVAMIND
TRAINING CENTER

NOVAMIND
CAMPUS

Formation Sensibilisation aux utilisateurs

Programme

06 64 43 94 73

novamind.fr

Contact
marie-lucie.delaistre@novamind.fr

NDA : 11757247775

Mis à jour le 17/05/2025

Informations pratiques

Objectifs

À l'issue de la formation "Cybersécurité : Sensibilisation aux utilisateurs" vous serez en mesure de :

• 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

Prérequis

• Maîtrise de l'outil informatique et de la langue française.

Public cible

• Salariés

Modalités pédagogiques

Tout au long de la formation, des temps théoriques alternent avec des temps pratiques. Des supports écrits sont transmis au stagiaire en versions numérique et papier.

En amont de la formation, un entretien téléphonique est réalisé pour définir les besoins et demandes des stagiaires afin que la formation corresponde au mieux.

• Présentiel : En appui des temps théoriques, un diaporama et un écran mural sont utilisés, tout en laissant place à une forte interactivité entre les stagiaires et les formateurs.

• Distanciel : Une solution à distance permettant la vidéo, le son, le partage d'écran, l'enregistrement des sessions, est utilisée : la formation est ainsi organisée sous la forme de classe virtuelle.

NOVAMIND
TRAINING CENTER

Informations pratiques

Modalités d'évaluation

- Un test de fin de formation (QCM, exercices, projet, présentation orale) est réalisé afin de valider les acquis.
- Une attestation de compétences validant les compétences acquises, non acquises et en cours d'acquisition sera remise à chaque stagiaire à l'issue de la formation.
- Chaque stagiaire est invité à participer à un bilan oral " à chaud complété par un questionnaire "à froid" envoyé quelques semaines plus tard, pour connaître l'impact de la formation suivie et d'en mesurer les apports au niveau professionnel.
- Une attestation de présence
- Dans le cas des formations à distance, un certificat de réalisation est délivré.

Formateurs

Experts dans le milieu de la cybersécurité

Modalités

Accessible en présentiel et distanciel

Tarif et financements

Financement personnel
960€ TTC

Durée

7 heures

NOVAMIND
TRAINING CENTER

Contenu

La sécurité informatique : comprendre les menaces et les risques

• Qu'entend-on par sécurité informatique (menaces, risques, protection) ?
• Comment une négligence peut-elle créer une catastrophe ?
• Réseaux d'entreprise (locaux, site à site, accès par Internet), quels enjeux ?
• Réseaux sans fil et mobilité : les applications à risques : internet, messagerie...
• Base de données et système de fichiers : menaces et risques
• Typologie des risques et vocabulaire (sniffing, spoofing, smurfing, hijacking...)

La protection de l'information et la sécurité du poste de travail

• Comprendre les contraintes liées au chiffrement
• Schéma général des éléments cryptographiques. Windows, Linux ou MacOs : quel est le plus sûr ?
• Gestion des données sensibles : comment les protéger ?
• 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 : comprendre l'intérêt de l'authentification renforcée
• Accès distant via Internet : comprendre les VPN

NOVAMIND
TRAINING CENTER

Contenu

Comment s'impliquer dans la sécurité du SI ?

- Analyse des risques, des vulnérabilités et des menaces
- Les contraintes réglementaires et juridiques
- La cybersurveillance et la protection de la vie privée
- La charte d'utilisation des ressources informatiques
- La sécurité au quotidien : comment avoir les bons réflexes ?

NOVAMIND
TRAINING CENTER