NOVAMIND
TRAINING CENTER

**NOVAMIND**
CAMPUS

# Formation
# Introduction à la Cybersécurité
## 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 « Introduction à la cybersécurité », vous serez en mesure de :

• Comprendre les principaux éléments qui assurent une sécurité dans l'utilisation des TIC (Technologies de l'Information et de la Communication) au quotidien
• Savoir identifier et signaler des activités malveillantes d'un type particulier

## Prérequis

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

## Public cible

• Salariés, demandeurs d'emploi, auto-entrepreneurs, étudiants

## 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
1 440€ TTC

## Durée

14 heures sur deux jours

NOVAMIND
TRAINING CENTER

# Contenu

## Les menaces

• Faire la différence entre les données et les informations
• Comprendre le terme : cybercriminalité
• Comprendre la différence entre hacker (hacking), cracker (cracking) et pirater dans un but éthique (ethical hacking)
• Connaître les menaces majeures pour la sécurité des données comme : les incendies, les inondations, les guerres, les tremblements de terre
• Connaître les menaces pour la sécurité des données causées par : les employés, le fournisseur d'accès, les personnes externes

## Valeur de l'information

• Comprendre pourquoi il est important de protéger les informations personnelles
• Comprendre pourquoi il est important de protéger des données commerciales sensibles
• Identifier les mesures à prendre pour empêcher les accès non- autorisés aux données comme : le cryptage des données, l'utilisation de mots de passe
• Comprendre les caractéristiques de base de la sécurisation de l'information
• Identifier les principales règles de protection, de conservation et de contrôle des données / données privées en vigueur dans votre pays
• Comment mettre en place des directives (lignes de conduite/guidelines) et des réglementations (policies) en matière d'utilisation des TIC

## Sécurité personnelle des fichiers

• Comprendre le terme : ingénierie sociale (social engineering) et ses implications comme : la collecte d'informations, la fraude, l'accès au système informatique
• Comprendre les effets de l'activation/la désactivation des macros dans les options de sécurité des applications
• Utiliser un mot de passe pour les fichiers comme : les documents, les fichiers compressés, les classeurs / feuilles de calculs
• Comprendre les avantages et les limites du cryptage des données

NOVAMIND
TRAINING CENTER

# Contenu

## Sécuriser et sauvegarder les données

• Connaître les méthodes pour s'assurer de la sécurité physique des dispositifs numériques mobiles
• Connaître l'importance de maîtriser la procédure de sauvegarde (backup) en cas de perte de fichiers, de données comptables, d'historique de navigation et de signets
• Identifier les paramètres d'une procédure de sauvegarde
• Sauvegarder des données

## Destruction des données sécurisées

• Savoir détruire de manière définitive des données qui se trouvent dans un lecteur ou dans un dispositif numérique mobile
• Connaître la différence entre un effacement et une totale destruction (définitive) de données
• Les méthodes habituelles de suppression définitive de données

NOVAMIND
TRAINING CENTER