RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

UniCamp

UNIVERSITÉ TOULOUSE III PAUL SABATIER

# MICROCERTIFICATION

## « Cybersécurité : Usages & Bonnes Pratiques »

**Direction de la Formation et de la Vie Universitaire**
**Université360**

# - SOMMAIRE -

## 2.1 Introduction

## 2.2 Objectifs pédagogiques

## 2.3 Contenu du programme

## 2.4 Méthodologie pédagogique

# TRA023-2 | Formation | Cybersécurité : Usages & bonnes pratiques

## 1.1 Introduction

Le programme de formation "sécurité informatique pour tous" vise à fournir aux participants un aperçu complet des principes et des meilleures pratiques de la sécurité informatique.

Il s'adresse à un large public qui souhaite :

- S’informer sur la cybersécurité,
- Connaître les enjeux de la sécurité informatique,
- Savoir protéger sa vie et son espace numérique

tant dans la vie personnelle que professionnelle.

Il aborde les concepts essentiels de la sécurité informatique et fournit des conseils pratiques pour se protéger contre les menaces et les attaques.

- Durée : 10 heures : 8 heures asynchrones (au rythme de 2 h par semaine), 2 heures synchrones (classe virtuelle) : 4 semaines de formation

- Dates : du 19 juin 2025 au 18 juillet 2025

## 1.2 Objectifs pédagogiques

- Identifier les principaux concepts et terminologies de la sécurité informatique.
- Reconnaître les menaces courantes auxquelles les utilisateurs informatiques sont confrontés.
- Appliquer les bonnes pratiques pour protéger ses données personnelles et sa vie privée.
- Mettre en place des mesures de sécurité pour ses appareils (ordinateurs, smartphones, tablettes, etc.).
- Expliquer les fondamentaux de la sécurité des réseaux et d'Internet.
- Reconnaître différents types d'attaques informatiques courantes et proposer des mesures de prévention.
- Mettre en place des mesures de sécurité des mots de passe et d'authentification.
- Appliquer les principes de base de la sécurité dans le cloud computing.
- Utiliser des compétences pratiques pour détecter et réagir aux incidents de sécurité informatique

## 1.3 Contenu du Programme

### 1.3.1 MODULE 0 : PRESENTATION DE LA FORMATION (SEMAINE 1)

- Attendus d'apprentissage
    - A l'issue de cette présentation, les participants seront en mesure de comprendre le cadre de la formation et ses objectifs
- Contenu :
    - Contextualiser la formation (à qui cela s'adresse le particulier et la personne en situation en entreprise)
    - Cas d'usages avec réactions inappropriées

### 1.3.2 MODULE 1 : INTRODUCTION A LA SECURITE INFORMATIQUE (SEMAINE 1)

- Attendus d'apprentissage :
    - À la fin de ce module, les participants devraient être en mesure d'expliquer les principaux concepts de base de la sécurité informatique et de comprendre l'importance de la sécurité informatique dans leur vie quotidienne et professionnelle.
- Contenu
    - Présenter les concepts de base de la sécurité informatique
    - Sensibiliser à Importance de la sécurité informatique dans la vie quotidienne

### 1.3.3 MODULE 2 : MENACES ET ATTAQUES INFORMATIQUES (SEMAINE 2)

- Attendus d'apprentissage :
    - Les participants devraient être capables de reconnaître et d'identifier les menaces et les attaques informatiques courantes, tels que le phishing, les logiciels malveillants et les ransomwares.
- Contenu
    - Lister les principales menaces et attaques courantes et leurs conséquences
        - DDOS
        - Usurpation d'identité
        - Ransomware
        - Vol d'infos
        - …
    - Illustrer des situations
        - Comment on s'en aperçoit
        - Comment cela arrive
        - Présenter en exemple des cas concrets (actualités, journaux, stats …)
        - …)

### 1.3.4 MODULE 3 : BONNES PRATIQUES, USAGES ET OUTILS (SEMAINE 3)

- Attendus d’apprentissage :
    - À la fin de ce module, les participants devraient être en mesure :
    - Appliquer les bonnes pratiques pour protéger leurs données personnelles,
    - Mettre en place des mesures de sécurité pour leurs appareils
    - Expliquer ce qu’est un réseau ?
    - Présenter les choix de sécurité dans l’usage des réseaux : VPN, navigation privée, protocoles sécurisés (https, imaps, ...)
    - Mettre en œuvre les bonnes pratiques pour créer des mots de passe forts, et d'appliquer ces mesures de sécurité dans leurs propres comptes en ligne.
    - Définir le concept d'authentification à deux facteurs
    - Assimiler les principes de base de la sécurité dans le cloud computing, savoir comment partager et stocker des données de manière sécurisée dans le cloud.
- Contenu :
    - Protection des données personnelles
        - Identifier et appliquer les bonnes pratiques pour protéger ses données personnelles
        - Mettre en œuvre la gestion des paramètres de confidentialité
    - Sécurité des appareils :
        - Sécuriser les ordinateurs, smartphones, tablettes, etc.
        - Déployer les mises à jour logicielles et antivirus
        - Sécurité des réseaux et d'Internet
        - Présenter la notion de réseau
        - Sécuriser sa navigation, ses transactions
    - Sécurité des mots de passe et authentification
        - Sensibiliser aux bonnes pratiques pour créer des mots de passe forts
        - Présenter les concepts Authentification à deux facteurs
        - Appliquer ces mesures de sécurité à ses propres comptes en ligne.
    - Sécurité dans le cloud computing
        - Présenter les principes de base de la sécurité dans le cloud
        - Partager et stocker des données de manière sécurisée dans le cloud

### 1.3.5 MODULE 4 : DETECTIONS ET REACTIONS AUX INCIDENTS DE SECURITE (SEMAINE 4)

- Attendus d'apprentissage
    - Être en mesure de reconnaître les signes d'une intrusion ou d'une compromission de la sécurité et de connaître les procédures de réponse aux incidents, y compris les étapes de détection, d'atténuation et de rapport.
- Contenu
    - Identifier les signes d'une intrusion ou d'une compromission de la sécurité
    - Présenter les procédures de réponse aux incidents :
        - Comment faire quand cela s'est produit.
        - Que ne pas faire

## 1.4 Méthodologie pédagogique

Le programme de formation sera animé par des formateurs expérimentés dans le domaine de la sécurité informatique.

Les modules combineront des présentations interactives, des démonstrations pratiques, des discussions de groupe et des exercices pratiques pour favoriser l'apprentissage actif et l'engagement des participants.

Des ressources complémentaires, telles que des documents de référence et des liens vers des outils et des ressources en ligne, seront également fournis pour approfondir les connaissances.

Évaluation : L'évaluation de la formation se fera à travers des quizzs périodiques tout au long du programme et un examen final.