CANDIDATURE

La sélection se fait en deux temps :

Admissibilité sur projet motivé détaillé mettant en avant l'engagement et l'expertise des candidats dans les disciplines enseignées

Admission après entretien avec un jury composé d'enseignants et de professionnels

MODALITÉS DE SÉLECTION

Information sur le site de l'IUT :
www.iut.u-bordeaux-montaigne.fr/etre-candidat/
Attention aux dates limites de téléchargement et de dépôt.

Pour en savoir plus, consultez le site de l'IUT.

www.iut.u-bordeaux-montaigne.fr

candidature, apprentissage, modalités de sélection, formation initiale, formation continue, formation en alternance, coût de la formation, organisation et contenu de la formation, journée «portes ouvertes», actualités…

IUT Bordeaux Montaigne
Formation continue
1 rue Jacques Ellul
33080 Bordeaux cedex - tél. 05 57 12 20 44

Secrétariat Formation continue
tél. 05 57 12 21 47
formation-continue-iut@iut.u-bordeaux-montaigne.fr

IUT BORDEAUX MONTAIGNE

Formation continue

Cybercriminalités : défis et enjeux humains

DIPLÔME UNIVERSITAIRE EN 1 AN

iut bordeaux montaigne

La singularité de ce diplôme en cybercriminologie réside dans son ancrage profond dans les sciences humaines et sociales, une démarche inédite en France. Ces enseignements sont soigneusement conçus et délivrés par des experts et chercheurs éminents de la cybersécurité et de la cybercriminalité.

INSERTION

À l'issue de la formation, les candidats doivent avoir pour objectif de se spécialiser dans un ou plusieurs domaines de la cybercriminalité / cybersécurité, en acquérant des compétences pointues, une compréhension approfondie des enjeux actuels, et une capacité à appliquer de solutions novatrices face à l'évolution constante des menaces numériques.

PUBLICS

Ce diplôme universitaire s'adresse à un public en formation continue.

Il est exclusivement ouvert aux candidats détenteurs de trois années d'expérience professionnelle pertinente en lien avec l'agir criminel (psychologue, avocat, magistrat, DSI, RSSI, DPO, analyste, agents des collectivités territoriales, chef d'entreprise, etc.) ou à défaut de l'obtention du certificat de remise à niveau proposé par l'E-Faculté de Psychologie et de Psychanalyse (EFPP) en criminalité.

La capacité d'accueil est de 20 places.

Ouverture de la formation sous réserve de 15 personnes inscrites. Possibilité au-delà de cette jauge d'inscrits de suivre les modules indépendamment donnant lieu à une certification.

OBJECTIFS PROFESSIONNELS

Le programme vise à renforcer les compétences professionnelles nécessaires pour relever les défis de la cybercriminalité / cybersécurité. En effet, l'accès généralisé à Internet, la diversification des canaux de communication, et la complexité des échanges numériques ont ouvert la porte à de nouveaux risques exploités par les cybercriminels. Au-delà de l'adoption de technologies avancées, ce DU se concentre sur la compréhension des comportements humains en situation de compromission ou d'atteinte, des motivations et des vulnérabilités individuelles ou collectives. La reconnaissance des différents types de cyber-risques auxquels sont confrontés entreprises, administrations, et particuliers est devenue une démarche fondamentale pour contrer cette forme de délinquance en constante évolution.

ORGANISATION

L'équipe est composée d'enseignants chercheurs français et étrangers, des membres des forces de l'ordre (gendarmerie et police), de professionnels œuvrant dans l'environnement de la lutte contre la cybercriminalité / cybersécurité.

Pour répondre aux besoins des apprenants, le programme du DU est conçu avec un module dispensé chaque mois, regroupant les participants pendant deux jours consécutifs, de novembre à juin (soit 8 modules / 8 mois de formation).

Les stagiaires doivent disposer d'un ordinateur personnel.

CONTENU

115 heures de cours

Les cours seront entièrement dispensés en présentiel.
Pour des raisons exceptionnelles, un mode hybride synchrone sera assuré permettant le cas échéant à l'apprenant de suivre deux modules en distanciel sur l'année.

Module 1 : Enquête au cœur de la cybercriminalité (18 heures)

Module 2 : Les recherches en sources ouvertes (12 heures)

Module 3 : La radicalisation en ligne (18 heures)

Module 4 : L'ingénierie sociale (14 heures)

Module 5 : Cyberharcèlement et violences en ligne (14 heures)

Module 6 : Crime organisé en ligne (17 heures)

Module 7 : Gestion de crise cyber (14 heures)

Module 8 : Colloque scientifique (8 heures)