Présentation

Objectifs

L'essor d'Internet a incontestablement accéléré et facilité les accès et les échanges de l'information. Cette fulgurante réussite dans la communication a favorisé l'apparition de nouvelles menaces criminelles. Ces menaces font courir des risques considérables pour les entreprises, les administrations publiques et les particuliers. La lutte contre la cybercriminalité est devenue un défi majeur mondial en raison de la dimension internationale de cette nouvelle délinquance souvent organisée.

La cybercriminalité évolue chaque jour, faisant apparaître de nouvelles formes de risques et de techniques de contournement de la loi, que le droit se doit de prendre en considération et auxquelles il doit s'adapter.

Le principal objectif de cette formation pluridisciplinaire est d'appréhender les différentes infractions et responsabilités liées à l'utilisation frauduleuse des réseaux numériques et des systèmes d'information..

Elle apporte aux étudiants, aux acteurs économiques, aux professionnels du droit, aux forces de l'ordre et à toutes les personnes confrontées à la cybercriminalité un éclairage sur :

- La nature des menaces liées aux réseaux numériques.
- Les dispositifs juridiques de lutte contre la cybercriminalité.
- Les techniques d'investigation numérique et les procédures d'établissement de la preuve.
- Les questions et les réponses juridiques qui se mettent en place aux plans national, européen et mondial

Programme

UE1 : Introductions aux réseaux et à l'Internet

(Mise à niveau technique)

- Organisation et structure physique des réseaux informatiques
- Caractéristiques techniques du réseau Internet (TCP/IP, DNS, WiFi..)
- RFID et réseaux de capteurs sans fils
- Caractéristiques des applications Web2.0 (réseaux sociaux, blogs, Twitter..)
- Les réseaux Peer to peer (P2P ou pair à pair)
- Caractéristiques et modes d'utilisation des outils de recherche sur Internet (moteurs, méta-moteurs, ..)
- Techniques de référencement
- Les fournisseurs de services de la société de l'information : rôles et catégories de services proposés

UE2 : Introduction au Droit et à la sécurité juridique

(Mise à niveau juridique)-

- Les différentes branches du droit
- Les systèmes juridictionnels français et européen
- Les droits et libertés fondamentaux
- Les diverses formes de responsabilité juridique

UE3 : Introduction aux aspects techniques de la sécurité des systèmes d'information et de la cybercriminalité

- Système d'information : définition, rôle et critères d'évaluation
- Cybercriminalité: menaces (piratage informatique, usurpation d'identité, e-réputation, "social engineering", fraudes, …)
- Introduction à la signature électronique et à la cryptologie
- Les systèmes de management de la sécurité de l'information
- Technologies de protection des réseaux sans-fil
- Normes de sécurisation d'un système d'information, RGS et PSSI
- Les acteurs de la sécurité de l'information
- Etude de cas.

UE4: Aspects juridiques et économiques de la sécurité des systèmes d'information

- Contexte juridique de la sécurité des systèmes d'information
- Les obligations légales, réglementaires de sécurisation
- Les enjeux de la sécurisation
- Les aspects juridiques de la démarche de sécurisation (cryptologie, chartes, préservation de la preuve, signalement des incidents...)
- La dématérialisation (contrats électroniques, preuve électronique, signature électronique...)
- Sécurité de l'information et intelligence économique

UE5 : Cybercriminalité: dispositifs juridiques jeux économiques et sociaux

- Panorama de la cybercriminalité (statistiques, évolution,...)
- Menaces et qualification juridique
- Acteurs et services Internet : qualification juridique
- Lutte contre la cybercriminalité et Droits et Libertés fondamentaux
- Instances de régulation, de prévention et de répression
- Cybercriminalité et coopérations nationales et internationales
- Droits et obligations des acteurs de la société de l'information
- Impact économique de la cybercriminalité (blanchiment d'argent, cyberfraudes, ..).
- Profil du Cyberdélinquant

UE6 : Informatique légale

- Introduction aux techniques d'investigation numériques (computer forensics)
- Panorama de la criminalistique
- Introduction à l'analyse criminelle opérationnelle

Modalités

CONDITIONS D'ADMISSION

Formation initiale :

Etudiants ayant validé une licence obtenue dans une université de l'espace européen ou un diplôme équivalent.
Un goût pour les nouvelles technologies ayant trait aux réseaux, à l'Internet et à l'investigation numérique est indispensable.

Formation continue :

Cette formation s'adresse aux professionnels qui souhaitent développer des compétences dans le domaine de la lutte contre la cybercriminalité. Elle permet de comprendre les enjeux de la sécurité de l'information et de la cybercriminalité, et d'en maîtriser les aspects juridiques".

Les professionnels peuvent ainsi valoriser l'expérience professionnelle qu'ils ont acquise, par l'obtention d'un diplôme universitaire.

Exemples de professionnels concernés par cette formation :

- Les salariés de l'industrie ou des collectivités locales qui sont responsables de la sécurité des systèmes d'information
- Le personnel chargé des enquêtes ou de leur supervision dans les affaires de criminalité informatique
- Les professionnels du droit amenés à traiter des dossiers liés à la cybercriminalité

Pré-requis : des connaissances de base sur les ordinateurs, les réseaux informatiques et Internet sont fortement conseillées. Un programme de mise à niveau technique et juridique (pour les étudiants et les professionnels non juristes ou non techniciens) est proposé avant le début de la formation.

CONDITIONS D'INSCRIPTION :

- Sélection sur dossier.
- **Retrait dossier candidature (Site UM1) à partir du 15 mai 2013**
- Date limite de dépôt de dossier: 25/10/2013
  - Capacité d'accueil limitée

Droits d'inscription :

- Professionnels: **1100 €**
- Etudiants: **240 €**
- **Calendrier des cours**
- Début des cours: **9 janvier 2014**
- Fin des cours **:** **4 juillet 2014**
- Volume horaire **100h** (+20h en option de mise à niveau technique et juridique)

RENSEIGNEMENTS ET RETRAIT DE DOSSIER

Département Informatique-Faculté de Droit et de Science politique

Adresse: 14, rue Cardinal de Cabrières
34060 MONTPELLIER CEDEX
Tél: 04 34 43 29 53
Courriel: adel.jomni@univ-montp1.fr

OU
Service Formation continue-Université Montpellier 1

Adresse: DIDERIS, Espace Richter,
Rue Vendémiaire, Bât. E - CS 29555
34961 Montpellier, cedex 2
Tél : 04 34 43 21 21-Fax : 04 34 43 21 90
Courriel: dideris@univ-montp1.fr

Faculté de droit

Université Montpellier 1

DIPLÔME D'UNIVERSITÉ

Cybercriminalité

Droit, Sécurité de l'information & Informatique légale

Directeur: **Adel Jomni: Enseignant-chercheur (UM1),**

Directeur du département Informatique-(DIRM) et formateur au sein de l'ECTEG (European Cybercrime Training & Education Group).

Coordination**: Estelle de Marco, Docteur en droit privé et sciences criminelles, spécialiste du droit de l'informatique et des réseaux.**

DÉPARTEMENT INFORMATIQUE & RESSOURCES MULTIMÉDIA

DYNAMIQUES DU DROIT