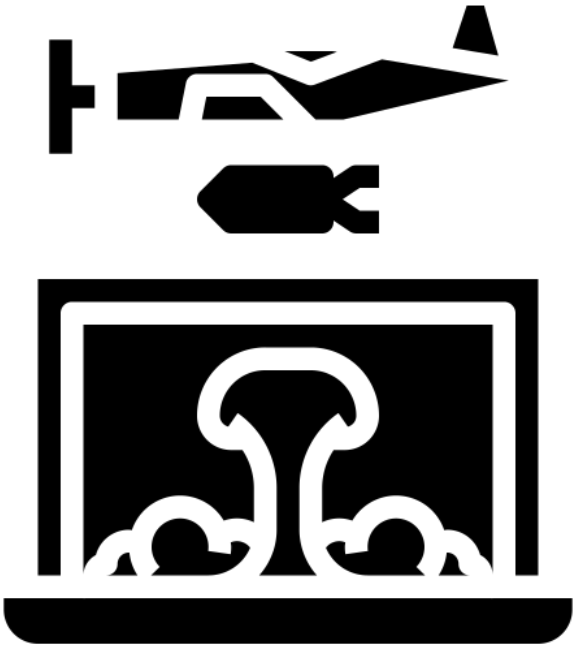
PLAN DE COURS | CRI3950L



Automne 2023

Criminalité informatique

Mardi de 13:00 à 16:00

Prof. David Décary-Hétu

david.decary-hetu@umontreal.ca | C-4071 | 514-343-6111 #3664

PLAN DE COURS | CRI3950L

CRIMINALITÉ INFORMATIQUE

DESCRIPTEUR DE COURS

Les changements technologiques au sens large ont amené une transformation dans les façons de commettre des crimes. Les auteurs mais aussi les agences d'application de la loi doivent maintenant tenir compte des éléments virtuels et dématérialisés afin d'évoluer dans ce nouveau contexte. Le présent cours se veut donc une introduction à cette nouvelle problématique.

OBJECTIFS DU COURS

Ce cours vise principalement à :

- Sensibiliser l'étudiant(e) à l'émergence et au développement de la criminalité informatique;
- Donner des outils théoriques et pratiques à l'étudiant(e) désireux (se) d'en apprendre davantage sur les crimes informatiques et;
- Comprendre les enjeux d'intervention pour les policiers en ce qui concerne les crimes commis sur internet.

PÉDAGOGIE ET ENSEIGNEMENT

Le cours est construit autour de présentations magistrales, mais contiendra aussi des exercices afin d'approfondir les connaissances sur le sujet. Il est attendu que les étudiants se préparent aux séances en lisant les textes associés à chaque cours.

ÉVALUATIONS

Les étudiants feront l'objet de deux évaluations.

Nature de l'évaluation	Pondération	Date
Mini-quiz après chaque cours	40%	À la fin de chaque cours
Examen final (travail pratique)	60%	15 décembre

Les cours auront lieu en présentiel. La présence au cours est nécessaire à la réussite de celui-ci. D'abord, les connaissances seront évaluées dans les mini-quiz qui auront lieu après chaque cours. Les informations importantes à savoir pour réussir les Mini-Quiz seront soulevées pendant le cours. Pour réussir le mini-quiz celui-ci doit être complété avant la fin du cours. Un temps sera accordé pour y répondre pendant les heures de cours. Il y aura

13 mini-quiz au courant de la session. Les 10 meilleurs résultats seront pris en considération pour la note. Il est donc possible de rater trois mini-quiz au courant de la session (par exemple pour une absence).

Finalement, l'examen final sera sous forme travail pratique. Une question sera donnée et les étudiants devront entreprendre une réflexion sur le sujet en faisant des liens avec la matière vue en classe. L'examen devra être remis avant minuit le 15 décembre 2023. Tout retard dans la remise des travaux entrainera une pénalité de 20% par période de 24h. Des consignes détaillées et des modalités d'évaluation seront disponibles sur Studium.

Les notes sont directement converties en lettre en fonction d'une logique de rang avec la grille de conversion **approximative** ci-dessous.

Grille de conversion des rangs (1er cycle)

Points	Note littérale	Valeur	Rang
4,3	A+	excellent	8%
4	A		25%
3,7	A-		
3,3	B+	Très bon	35%
3	B		
2,7	B-		
2,3	C+	bon	25%
2	C		
1,7	C-		0-7%
1,3	D+	passable	
1	D		
0	E	échec	0%

DÉROULEMENT DU COURS

Cours 1: Introduction | 5 septembre

Présentation du cours

Présentation des évaluations

Concepts importants en criminalité informatique

- Cassuto, T. (2018). "Nouvelles perspectives dans la lutte contre la cybercriminalité." *Sécurité globale*. 15(3): 29-35.

Cours 2: Droit et informatique | 12 septembre

Usages problématiques et criminels d'internet

Droit et informatique

- Ellyson, L. (2019). "La saisie de données informatiques en droit criminel canadien." *Canadian Criminal Law Review*. 24(1): 79-110.

Cours 3: Technologies 1 | 19 septembre

Technologies qui permettent la cybercriminalité

Darkweb

Chiffrement

- Tréguer, F. (2019). "Anonymat et chiffrement, composantes essentielles de la liberté de communication." DANS Van Enis, Q & De Terwangne, C. *L'Europe des droits de l'homme à l'heure d'Internet*. Bruxelles, Belgique : Bruylant.

Cours 4: Technologies 2 | 26 septembre

Technologies qui permettent la cybercriminalité

Cryptomonnaies

- Desbois, D. (2023). "Crypto-actifs: déboires financiers, turpitudes juridiques et réglementations lacunaires." *Terminal: Technologie de l'information, culture & société*. (136).

Cours 5: Trafics illicites | 3 octobre

Vente de drogue sur internet

Trafics illégaux sur le darkweb

Cryptomarchés

- Fraser, I., Chauvin, G. S., Faubert, C., & Décary-Hétu, D. (2021). “Les interventions policières sur les facilitateurs du crime.” *Criminologie*. 54(2): 295-320.

Cours 6: Piratage informatique | 10 octobre

Botnets

Ransomware

Virus, vers et code malicieux

Piratage

- Lagare, S. (2021). ”Études des cyberattaques de type ransomware et proposition de solutions adaptées aux particuliers et PME.”Thèse de doctorat. Haute école de gestion de Genève.

17 octobre : semaine de lecture

Cours 7: Fraude informatique | 24 octobre

Sécurité informatique

Spam

Fraude

- Guillot, M., & Décary-Hétu, D. (2019). ”Cryptomarchés et carding: impact sur l’offre et la demande.” Criminologie. 52(2): 63-82.

Cours 8: Propagande informatique | 31 octobre

Propagande haineuse

Hacktivisme

Extrémistes en ligne au Canada

- Badouard, R. (2020). "La régulation des contenus sur Internet à l'heure des «fake news» et des discours de haine." *Communications*. (1): 161-173.

Cours 9: Conférencier invité | 7 novembre

À déterminer selon les intérêts des étudiants.

Cours 10: Délinquance sexuelle 1 | 14 novembre

Pornographie juvénile

- Paquette, S., Bergeron, A., et Fortin, F. (2020). "Matériel d'exploitation sexuelle d'enfants sur Internet: étendue du phénomène, auteurs d'infractions et enjeux légaux." Dans Fortin, F. (Éd.) *Cybercrimes et enjeux technologiques : contexte et perspectives*. Montréal, Canada: Les Presses Internationales Polytechnique.

Cours 11 : Délinquance sexuelle 2 | 21 novembre

Leurre informatique

- Paquette, S., Bergeron, A., et Fortin, F. (2020). "Sollicitation à des fins sexuelles : un état de la question sur le leurre d'enfant par voie informatique." Dans Fortin, F. (Éd.) *Cybercrimes et enjeux technologiques : contexte et perspectives*. Montréal, Canada: Les Presses Internationales Polytechnique.

Cours 12: Cybercriminalité et les jeunes | 28 novembre

Cyberintimidation

Jeux vidéo

Autres problématiques touchant les jeunes.

- Blécot, L., Lakrary, A., Laloux, M., & Kempeneers, P. (2022). "L'échange de nudes chez les jeunes français et belges francophones de 13–25 ans: une étude exploratoire." *Sexologies*. 31(3): 147-155.

Cours 13: Attaques informatiques par des États-nations | 5 décembre | Local 3120

Espionnage économique

Cyberwarfare

Cyberattaque dans les élections.

📖 Cattaruzza, A. (2019). "De la guerre à la cyberguerre ?" Dans Cattaruzza, A. (Éd.). *Géopolitique des données numériques: Pouvoir et conflits à l'heure du Big Data*. Paris, France: Le Cavalier Bleu.

MATÉRIEL REQUIS

Aucun matériel n'est requis pour le cours.

STUDIUM

Studium (https://studium.umontreal.ca) sera la plate-forme privilégiée pour échanger des informations et des documents. Studium vous permettra de télécharger les notes de cours, de télécharger des guides supplémentaires aux notes de cours, de télécharger les consignes pour les évaluations et aussi de déposer les évaluations. Pour avoir accès à Studium, l'étudiant doit être dûment inscrit à l'Université et être détenteur d'un UNIP.

CAPTATION VISUELLE OU SONORE

L'enregistrement de ce cours, en tout ou en partie, et par quelque moyen que ce soit, est interdit à moins d'en avoir obtenu l'autorisation préalable de la part de la chargée de cours ou du chargé de cours. L'autorisation d'enregistrement n'entraîne d'aucune façon la permission de reproduction ou de diffusion sur les médias sociaux ou ailleurs des contenus captés. Ces dernières sont interdites sous toutes formes et en tout temps.

RENSEIGNEMENTS ET RÈGLEMENTS D'ÉTUDES AU PREMIER CYCLE

Site web de l'École de criminologie

Nous vous invitons à consulter le guide étudiant de votre programme.

Nous vous invitons aussi à consulter le règlement pédagogique.

JUSTIFICATION D'UNE ABSENCE

L'étudiant doit motiver, par écrit, toute absence à une évaluation ou à un cours faisant l'objet d'une évaluation continue dès qu'il est en mesure de constater qu'il ne pourra être présent à une évaluation et fournir les pièces justificatives. Dans les cas de force majeure, il doit le faire le plus rapidement possible par téléphone ou courriel et fournir les pièces justificatives dans les cinq jours ouvrés suivant l'absence. Le doyen ou l'autorité compétente détermine si le motif est acceptable en conformité des règles, politiques et normes applicables à l'Université.

Les pièces justificatives doivent être dûment datées et signées. De plus, le certificat médical doit préciser les activités auxquelles l'état de santé interdit de participer, la date et la durée de l'absence, il doit également permettre l'identification du médecin. À noter que l'étudiant doit remplir le formulaire et le remettre au responsable ou au TGDE de son programme.

PLAGIAT ET FRAUDE

La politique sur le plagiat et la fraude sont applicables à toutes les évaluations prévues dans ce cours. Tous les étudiants sont invités à consulter le site web http://www.integrite.umontreal.ca/ et à prendre connaissance du Règlement disciplinaire sur le plagiat ou la fraude concernant les étudiants. Plagier peut entrainer un échec, la suspension ou le renvoi de l'Université.

RÉVISION DE L'EXAMEN FINAL

Au plus tard 21 jours après l'émission du relevé de notes, l'étudiant qui, après vérification d'une modalité d'évaluation a des raisons sérieuses de croire qu'une erreur a été commise à son endroit peut demander la révision de cette modalité en adressant à cette fin une demande écrite et motivée au doyen ou à l'autorité compétente de la faculté responsable du programme auquel il est inscrit. Si le cours relève d'une autre faculté, la demande est acheminée au doyen ou à l'autorité compétente de la faculté responsable du cours. À noter que l'étudiant doit remplir le formulaire et le remettre au responsable ou au TGDE de son programme.

RÉFÉRENCES PERTINENTES

Brenner, S. W. (2007). "Cybercrime: Re-thinking crime control strategies." Jewkes, Y. (Ed.) *Crime Online*. Portland, USA: Willan.

Britz, M.T. (2009). *Computer forensics and cybercrime: An introduction. 2d ed.* Upper Saddle River, NJ: Prentice Hall.

Dolan, K.M. (2004). "Internet auction fraud: The silent victims." *Journal of Economic Crime Management*. 2(1): 1–22.

Finn, J. (2004). "A survey of online harassment at a university campus." *Journal of Interpersonal Violence*. 19(4): 468–483.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Boston, USA: Addison-Wesley.

Jordan, T. et Taylor P. (2004). *Hacktivism and cyberwars: Rebels with a cause?* London, UK: Routledge.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Garden City, USA: Anchor Doubleday.

McQuade, S. C. (2006). *Understanding and managing cybercrime*. Boston: Allyn and Bacon.

Newman, G.R., et Clarke, R.V. (2003). *Superhighway robbery: Preventing e-commerce crime*. Portland, USA: Willan.

Olson, P. (2013). *We Are Anonymous*. New York, USA: Random House.

Quayle, E. et Taylor, M. (2002). "Child pornography and the Internet: Perpetuating a cycle of abuse." *Deviant Behavior*. 23:331–361.

Quayle, E. et Taylor, M. (2003). *Child pornography: An Internet crime*. New York, USA: Routledge.

Stambaugh, H., Beaupre, D. S. Icove,D. S. Baker, Cassady, W. et Williams, W.P. (2001). "Electronic crime needs assessment for state and local law enforcement." U.S. Department of Justice.

Taylor, P.A. (1999). *Hackers: Crime in the digital sublime*. New York, USA: Routledge.

Taylor, R. W., Caeti,T.J., Loper,D.K., Fritsch, E. J. et Liederbach, J. (2006). *Digital crime and digital terrorism*. Upper Saddle River, USA: Pearson Prentice Hall.

Wall, D. (2001). *Crime and the Internet*. New York, USA: Routledge.