Plan de cours

CF100 - Cyberfraude

Programme des certificats
Été 2025
3 Crédits
3-0-6
www.moodle.polymtl.ca

Chargés de cours

Nom	**Abdelwahab Laouni**
Courriel	abdelwahab-2.laouni@polymtl.ca

Description du cours

Introduction à la cyberfraude. Défis liés à l'utilisation de l'intelligence artificielle, l'internet des objets et l'informatique quantique. Différents types de cyberfraude, outils et méthodes utilisés par les cybercriminels. Moyens de protection contre les menaces. Utilisation des technologies de l'intelligence artificielle, l'internet des objets et de la cryptographie de l'informatique quantique pour améliorer la cybersécurité des systèmes d'information. Valeur économique de la sécurité informationnelle. Fonctionnement et financement des réseaux de cybercriminels et leurs méthodes de protection. Meilleures pratiques pour se protéger contre la cyberfraude. Lois et les réglementations. Impact sur la réputation des entreprises et la confiance des consommateurs : perceptions et réalité.

COURS PREALABLES	COURS COREQUIS	COURS SUBSEQUENTS
-	-	-

Objectifs d'apprentissage

À la fin du cours, l'étudiant sera en mesure :

- Reconnaître les différents types de cyberfraude et les tendances actuelles ;
- Identifier et décrire les techniques de cyberfraude ;
- Expliquer les enjeux économiques de la cyberfraude ;
- Interpréter et démontrer les relations entre la confiance, la réputation, les consommateurs, les entreprises et les fraudeurs ;

- Formuler des pistes de solutions pour faire face à la cyberfraude qui évolue en fonction des nouvelles technologies, des comportements des utilisateurs et des attaques de plus en plus sophistiquées ;
- Nommer et décrire les notions de la gestion de risques ainsi que les lois, réglementations et standards généralement associés au commerce électronique et affectant la cyberfraude ;
- Identifier les nouvelles stratégies de fraudes avec l'IA et la chaîne de blocs (Blockchain) ;
- Reconnaitre les nouvelles menaces de la cyberfraude en utilisant la cryptographie de l'informatique quantique, l'IA, l'IdO et l'IIdO.

Matériel Requis

Processeur : Intel I5 8e génération ou mieux ou AMD Ryzen 5 Mobile Processor
Disque dur/Stockage : SSD 512Go ou mieux
Mémoire vive : 8Go ou mieux

Carte graphique : Rien de particulier, la carte graphique intégrée suffit
Système d'exploitation : Windows 10 ou 11
Autres : Suite Office de base, Connexion Internet avec une vitesse minimale de 30Mbps

ATTENTION ! les processeurs ARM (M1, M2) d'Apple par exemple créent des problèmes avec les cours et ne sont pas recommandés

À noter que les besoins en bande passante peuvent varier en fonction de la densité de l'expérience multimédia. Cependant, il est fortement recommandé d'avoir une connexion haute vitesse standard (5 Mb/s) afin de profiter pleinement de l'expérience Zoom.

- Webcam.
- Microphone – casque d'écoute (connecteur USB recommandé).

Pour plus de détails, voir les liens suivants :
https://www.polymtl.ca/si/outil-de-visioconference-zoom
https://support.zoom.us/hc/fr/articles/201362023-Zoom-system-requirements-Windows-macOS-Linux#h_d278c327-e03d-4896-b19a-96a8f3c0c69c

Méthodes d'enseignement et d'apprentissage

Cours offert par Internet seulement synchrone ou asynchrone.

Quelques éléments de réflexion entourant l'utilisation de systèmes d'intelligence artificielle (IA) générative (ex : ChatGPT, OpenAI Codex, GitHub Copilot, DALL-E, Midjourney, etc.) qui sont à préciser :
• Ces outils peuvent être utilisés pour l'aide à l'apprentissage.
• Ils ne sont pas permit dans les évaluations (devoirs, examens, projet).
• Les personnes étudiantes ne sont pas autorisées de verser le matériel de cours dans un système de type ChatGPT pour en faire un résumé.

Les personnes étudiantes qui décident d'utiliser des systèmes d'intelligence artificielle générative sont avisées des risques suivants :
• La fiabilité des réponses ;
• La fraude et le plagiat ;
• La confidentialité des données et le respect du droit d'auteur.

Format des travaux

La présentation orale devra être soumise par Moodle en suivant les instructions données en cours ou être en présentiel au cours virtuel.

Remise des travaux d'équipe

Le travail d'équipe peut être effectué en équipe de 2 et les détails seront expliqués dans le cadre du cours.

Critères d'évaluation

Les critères d'évaluation seront disponibles dans Moodle Cours 1.

Personnes-ressources

Support aux étudiants : certificats@polymtl.ca
Support technique : support.certificat@polymtl.ca
Support Zoom : support.certificat@polymtl.ca
Service aux étudiants – Soutien à la réussite : https://www.polymtl.ca/soutien/
Soutien aux étudiants en situation de handicap : https://www.polymtl.ca/soutien/accueil-des-etudiants

Documentation

Pour la documentation concernant le cours, consulter Moodle.
Lectures suggérées

Mandiant. (2013) APT1: Exposing One of China's Cyber Espionage Units. États-Unis.
Tiré de : https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
Ozkaya, E., & Aslaner, M. (2019). Hands-on cybersecurity for finance. Tiré de :
https://www.packtpub.com/networking-and-servers/hands-cybersecurity-finance
Black, D., & Stewart Olsen, C. (2018). Les Cyberattaques – Elles devraient vous empêcher de fermer l'oeil, Canada.
Tiré de :https://sencanada.ca/content/sen/coXmmittee/421/BANC/Reports/BANC_Report_FINAL_f.pdf .
Ozkaya, E., & Aslaner, M. (2019). Hands-on cybersecurity for finance. Tiré de :
https://www.packtpub.com/networking-and-servers/hands-cybersecurity-finance
Black, D., & Stewart Olsen, C. (2018). Les Cyberattaques – Elles devraient vous empêcher de fermer l'oeil, Canada.
Tiré de : https://sencanada.ca/content/sen/committee/421/BANC/Reports/BANC_Report_FINAL_f.pdf .
• Akhgar, B., & Brester, B. (2016). Combatting Cybercrime and Cyberterrorism : Challenges, Trends and Priorities.Suisse. Springer.
• Association of Certified Fraud Examiners. (2016). Report to the nations on occupational Fraud and Abuse.
Tiré de : http://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf
• Cusson, M. Dupont, B. & Lemieux, F. (2007) Traité de sécurité intérieure. Montréal, Québec. Les Éditions Hurtubise HMH ltée.
• Goodman, M. (2016) Future Crimes. États-Unis. First Anchor Books.
• Hernandez, E., Regaldo, D. & Villeneuve, N. (2015) An Inside Look: Into the world of Nigerian scammers. États-Unis. FireEye Labs.
• Krebs, B. (2014). Spam Nation. Naperville, Illinois, États-Unis. Soucebooks.
• Seely, B. (2016) Cyber Fraud: the web of lie. Washington, États-Unis. Seely Secuirty.
• TZU, S. (1999). L'art de la guerre. Paris : Flammarion.

Sites Internet d'intérêt

Centre antifraude du Canada — http://www.antifraudcentre.ca
Federal Bureau of Investigation — Internet Crime Complaint Center (IC3) — https://www.ic3.gov
Gendarmerie Royale du Canada — http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm
Association of Certified Fraud Investigators (ACFE) — http://www.acfe.com/
Lectures additionnelles annoncées lors du cours.

Programme du cours

Cours et Dates	Thèmes	Activités	Évaluation
Cours 1 : 7 mai	Présentation du cours et de ses objectifs. Mode d'évaluation. Définition de la cyberfraude. Introduction, historique de la cyberfraude et tendances actuelles.	Cours magistral.	
Cours 2 : 12 mai	Menaces de Cyberfraude : les meilleures pratiques pour protéger les systèmes d'information contre l'hameçonnage, malware, rançongiciel, et autres attaques.	Cours magistral.	
Cours 3: 14 mai	L'intelligence artificielle et la Cyberfraude : les risques dans les systèmes de sécurité, les défenses contre et les attaques liées à l'utilisation de l'IA.	Cours magistral	
19 mai	**Journée sans cours ni examen– Semaine de relâche**		
Cours 4: 21 mai	Blockchaine et Cyberfraude : utilisation de cette nouvelle technologie afin de commettre des crimes numériques.	Cours magistral.	
Cours 5 : 26 mai	L'Internet des objets (IdO) et la Cyberfraude : les risques liés à la connectivité accrue des IdO ; Les vulnérabilités courantes des appareils IdO et les mesures de sécurité pour protéger les données.	Cours magistral.	
Cours 6 : 28 mai	Vol et usurpation d'identité. Mécanismes d'authentification. Sécurité de l'information. Propriété intellectuelle. Lois et réglementation en matière de vie privée. Droit à l'oubli. Éthique et vie privée.	Cours magistral.	
Cours 7 : 2 juin	***Contrôle périodique***		***CP01***
Cours 8 : 4 juin	Cyberfraude dans les milieux financiers, de la santé et de l'énergie : escroquerie en ligne, vol d'identité, blanchiment d'argent. Les multiples couches du web : la surface, le web profond et le web noir. L'économie de la Cyberfraude.	Cours magistral.	
Cours 9 : 9 juin	La cybersécurité pour les entreprises et les individus : les meilleures pratiques pour protéger les données commerciales et personnelles, les politiques de sécurité des données et les processus de récupération d'urgence	Cours magistral.	
Cours 10 : 11 juin	La cybersécurité pour les gouvernements : les risques pour la sécurité nationale, les politiques de cybersécurité pour les agences gouvernementales et les partenariats public-privé pour lutter contre la Cyberfraude.	Cours magistral.	
Cours 11[(1)] : 16 juin	Les tendances futures de la cyberfraude. Révision et préparation à l'examen final.	Cours magistral.	

Cours et Dates	Thèmes	Activités	Évaluation
Cours 12 : 18 juin.	Présentation des travaux de session.		PO01
Cours 13 : 23 juin	***Examen Final***		***EF01***

ÉVALUATION

NATURE	NOMBRE	MODE DE RÉALISATION (Individuel/équipe)	PONDÉRATION	DATE
Contrôle périodique (CP01)	1	Informatisé : en ligne, à livre fermé ou avec restrictions, par activité « Test » MoodleExamen et surveillance avec Proctor Exam et/ou Lab. Info.	40 %	2 juin
Présentation orale (PO01)	1	Vidéoconférence ou enregistrement vidéo (2) .	15 %	18 juin
Examen final (EF01)	1	Informatisé : en ligne, à livre fermé ou avec restrictions, par activité « Test » MoodleExamen et surveillance avec *Proctor Exam* et/ou *Lab. Info*.	45 %	23 juin

(1) Dernière séance pour procéder à l'Évaluation de l'enseignement » par les étudiants.

(2) Dépôt des vidéos : les enregistrements vidéo des étudiants **ne doivent PAS être déposés sur Moodle pour des raisons de capacité**. Les étudiants peuvent utiliser une **plateforme vidéo (YouTube**) et communiquer l'hyperlien sur Moodle.

Charge de travail

Présence en cours : 11 périodes de 3 h + contrôle périodique & examen final = 39 h
Travail personnel : étude personnelle : lecture et étude 36 h ; heures dédiées au projet 17 h ; préparation aux tests et à l'examen final 40 h = 93 h
Total : 132 h

*** Cette information est donnée à titre indicatif seulement. Certaines personnes peuvent avoir besoin d'investir plus ou moins de temps.

Mode d'enseignement à distance

L'enseignement et l'encadrement du cours sont en mode synchrone & asynchrone. Les séances seront enregistrées et disponibles pendant la durée du trimestre en entier.

Mention relative à la protection des renseignements personnels : enregistrement des activités d'enseignement en ligne en mode synchrone

Les activités d'enseignement en ligne en mode synchrone seront enregistrées afin de permettre aux personnes étudiantes ne pouvant pas assister en temps réel au cours d'avoir accès à l'activité d'enseignement. L'enregistrement sera ensuite rendu disponible sur Moodle aux seules personnes étudiantes inscrites à ce cours au présent trimestre.

Si l'étudiante ou l'étudiant active son micro et sa caméra lors de cette activité d'enseignement, il est possible que son nom, son image et sa voix apparaissent sur l'enregistrement. Ces renseignements personnels seront accessibles à la personne enseignante, aux personnes étudiantes inscrites à ce cours au présent trimestre et aux employés de Polytechnique affectés à la gestion de Moodle. L'enregistrement sera conservé de façon confidentielle conformément à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1.

L'enregistrement sera retiré de Moodle à la fin de la session et sera détruit dans les 30 jours après la fin de la session.

Si l'étudiante ou l'étudiant ne souhaite pas être enregistré, il est de sa responsabilité de désactiver son microphone et sa caméra.

À défaut de désactiver son microphone et sa caméra, l'étudiante ou l'étudiant consent à l'enregistrement audio ou audiovisuel, à la conservation, à l'utilisation et à la rediffusion de l'enregistrement de son nom, de sa voix et de son image dans le cadre de l'activité d'enseignement en ligne

Rappel : droit d'auteur

Les activités d'enseignement en ligne sont protégées par les droits d'auteur et le droit à la vie privée, dont le droit à l'image. En conséquence, la personne étudiante ne peut pas :

- Partager les vidéos ou des extraits de celles-ci avec une autre personne ;
- Diffuser ou vendre les vidéos.

Fraude : règlement et sanctions

Les étudiantes et les étudiants doivent adopter une attitude professionnelle exemplaire. L'article 9 des règlements des études aux certificats présente la position de Polytechnique Montréal à l'égard de la fraude sur la base du principe de tolérance zéro. Voici quelques éléments tirés du règlement en vigueur.

Par fraude, on entend toute forme de plagiat, de tricherie ou tout autre moyen illicite utilisé par une étudiante ou un étudiant pour obtenir un résultat d'évaluation non mérité ou pour influencer une décision relative à un dossier académique.

À titre d'exemple, constituent une fraude :

- L'utilisation totale ou partielle, littérale ou déguisée, d'une œuvre d'autrui, y compris tout extrait provenant d'un support électronique, en le faisant passer pour sien ou sans indication de référence à l'occasion d'un examen, d'un travail ou de toute autre activité faisant l'objet d'une évaluation ;
- Le non-respect des consignes lors d'un contrôle, d'un examen, d'un travail ou de toute autre activité faisant l'objet d'une évaluation ;
- La sollicitation, l'offre ou l'échange d'information pendant un contrôle ou un examen ;
- La falsification de résultats d'une évaluation ou de tout document en faisant partie ;
- La possession ou l'utilisation pendant un contrôle ou un examen de tout document, matériel ou équipement non autorisé y compris la copie d'examen d'une autre personne étudiante.

Selon la gravité de l'infraction et l'existence de circonstances atténuantes ou aggravantes, l'étudiante ou l'étudiant peut se voir imposer une sanction correspondant à, entre autres, l'attribution de la cote 0 pour l'examen, le travail ou toute autre activité faisant l'objet d'une évaluation qui est en cause, l'attribution de la note F pour le cours en cause, l'attribution de la note F à tous les cours suivis au trimestre.

Dans le cas d'un travail en équipe, les étudiantes et les étudiants d'une même équipe de travail tel que reconnu par l'enseignant sont solidaires du matériel produit au nom de l'équipe. Si un membre de l'équipe produit et remet un travail au nom de l'équipe et qu'il s'avère que ce travail est frauduleux tous les membres de l'équipe sont susceptibles de recevoir une sanction à moins qu'il soit démontré sans ambiguïté que l'infraction est le fait d'un ou de quelques membres de l'équipe en particulier.

Ressources et services pour les étudiantes et étudiants

Le Service aux étudiants (SEP) est constitué de professionnels qualifiés et d'une Escouade étudiante, dédiés à favoriser votre bien-être et votre réussite à Polytechnique Montréal, autant sur le plan académique, personnel que social. Que ce soit sous la forme de rencontres individuelles, d'ateliers pratiques ou de programmes tels que le tutorat et le mentorat, les services offerts vous aideront à vous épanouir à votre plein potentiel durant vos études à Polytechnique Montréal. N'hésitez pas à les contacter. Vous avez tout à y gagner !

Le Bureau d'intervention et de prévention des conflits et de la violence (BIPCV), vous accueille, vous guide et vous soutient en matière de violence à caractère sexuel, harcèlement ou tout enjeu relatif au respect des personnes. Le BIPCV est un bureau indépendant, assurant un service respectant la confidentialité et une écoute sans jugement. Contactez-les : bipcv@polymtl.ca 514 340 4711 Poste 5151.