

Sigle : CYB1073 Gr. 01**Titre : Cybersécurité comportementale****Session : Automne 2026 Horaire et local****Professeur : Caissy, David****1. Description du cours paraissant à l'annuaire :****Objectifs**

Au terme de ce cours, l'étudiant.e sera en mesure de comprendre les principaux facteurs humains de risques en cybersécurité et de décrire différentes techniques d'ingénierie sociale et les mécanismes d'influence sur lesquels ils s'appuient.

Contenu

Éléments de base de cybersécurité. Facteurs humains de risque en cybersécurité : erreurs et négligence, limitations et biais cognitifs. Profilage des cyberattaquants et des cyber-défenseurs : motivations, comportements. Ingénierie sociale : mécanismes d'influence, tromperie, éléments de théorie des jeux comportementale. Risques liés aux médias sociaux et santé mentale : phénomènes de bulles, désinformation, cyberintimidation, pédo-piégeage. Problématiques psychologiques et sociales liées aux mécanismes d'authentification, choix et réutilisation des mots de passe, acceptabilité sociale de la biométrie. Techniques défensives basées sur le comportement (pots de miel, stéganographie, etc.).

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

Compréhension de l'importance des différents aspects reliés aux facteurs de risques humains dans la cybersécurité. Clairement identifier les attaques par hameçonnage et par ingénieries sociale. Être en mesure de comprendre et d'expliquer les risques reliés à une utilisation non sécuritaire des media sociaux. Se familiariser avec les techniques d'analyses comportementales pour la détection des menaces en cybersécurité.

3. Stratégies pédagogiques :

Il s'agit d'un cours magistral en mode **non-présentiel avec deux examens en présentiel**. Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours.

Les étudiant(e)s qui s'inscrivent à ce cours doivent s'assurer qu'ils ont :

- **Microsoft Teams.** Un guide d'utilisation de Microsoft Teams est disponible sur le site de l'UQO : <https://uqo.ca/guide-utilisateurs/formation-video-microsoft-teams>
- Une connexion Internet, une webcam et un microphone.
- La suite **Office 365** (les étudiant(e)s ont un accès gratuit à la suite Office 365 : <https://uqo.ca/sti/outils-numeriques>).

4. Heures de disponibilité ou modalités pour rendez-vous :

Période de consultation sur rendez-vous seulement par courriel : david.caissy@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Introduction • Cybersécurité comportementale • Concepts de base de la sécurité de l'information • Modélisation des menaces	10 sept. 2026
2	Éléments de base en cybersécurité • Composantes réseaux • Zones et niveaux d'accès • Mécanismes de prévention et de détection des cyberattaques	17 sept. 2026

3	Cyberattaques contre les organisations • Vecteurs d'attaque • Attaques côté client • Commandement et contrôle (C2)	24 sept. 2026
4	Facteurs humains de risques en cybersécurité • Erreurs et négligence • Limitations et biais cognitifs • Comportements des utilisateurs • Théorie des jeux comportementale	1 oct. 2026
5	Ingénierie sociale • Mécanismes d'influence et de tromperie • Relation de confiance • Études de cas • Phishing (hameçonnage) • Appâtage • Chantage et extorsion Devoir 1 : Hameçonnage ciblé	8 oct. 2026
6	Semaine d'études	15 oct. 2026
7	Organisation et gouvernance • Meilleures pratiques • Séparation des responsabilités et des pouvoirs • Formation aux employés	22 oct. 2026
8	Examen de mi-session (en présentiel)	29 oct. 2026
9	Médias sociaux • Phénomènes de bulles • Désinformation • Cyberintimidation • Pédo-piégeage	5 nov. 2026
10	Intelligence artificielle (IA) et facteurs de risques humains • IA générative • Surcharge d'informations • Érosion de la pensée critique • Ingénierie sociale assistée par l'IA	12 nov. 2026
11	Facteurs humains dans le choix de mots de passe • Politiques de sécurité • Choix et réutilisation de mots de passe • Attaques contre les mots de passe	19 nov. 2026
12	Mécanismes d'authentification • Identification, authentification et autorisation • Facteurs d'authentification • Authentification unique • Mécanismes robustes contre les techniques d'hameçonnage Devoir 2 : Programme de sensibilisation à la cybersécurité comportementale	26 nov. 2026
13	Techniques défensives • Pots de miel • Stéganographie • Détection des menaces internes	3 déc. 2026

14	Techniques d'analyses comportementales - Analyse des comportements des utilisateurs et entités - Corrélation d'événements - Détection d'anomalies et évaluation du risque comportemental - Modification de l'accès basé sur le comportement (ABAC)	10 déc. 2026
15	Examen final (en présentiel)	17 déc. 2026

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs du cours. Dans le cas spécifique du cours **Cybersécurité comportementale**, l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session (en présentiel) : 35 %**
- **Examen final (en présentiel) : 40 %**
- **Devoir 1 : 15%**
- **Devoir 2 : 10%**

7. Politiques départementales et institutionnelles :

- Politiques relatives à la tenue des examens
- Note sur le plagiat et les fraudes
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance **ZÉRO** en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.

Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.

Ensemble, participons à une culture de respect.

Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

NOTES DE COURS : Disponibles via Moodle.

Références recommandées pour le cours :

Solange Ghernaouti, *Cybercriminalité - Comprendre. Prévenir. Réagir*. ISBN: 978-2-10-085869-9

Christopher Hadnagy, *Social Engineering - The Science of Human Hacking*. ISBN: 978-1-119-43338-5

9. Page Web du cours :

<https://moodle.uqo.ca/course/view.php?id=49848>