niversité du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB1073 Gr. 01
Titre : Cybersécurité comportementale
Session : Automne 2022 **Horaire et local**
Professeur : Touati, Hedi

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 non présentiel et des travaux individuels et d'équipe.

Les étudiant(e)s qui s'inscrivent à ce cours doivent s'assurer qu'ils ont : un ordinateur (avec un système d'exploitation Windows); une connexion Internet; une webcam; 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).

Guide d'utilisation de Zoom à l'intention des étudiants

Site pour soutien de réussite en mode non-présentiel : uqo.ca/etudier-non-presentiel.

Nota : On pourra vous demander d'installer quelques logiciels selon les activités, mais il s'agira de logiciels gratuits.

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

Période de **consultation** sur **rendez-vous**

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Introduction et rappels : éléments de base de cybersécurité.	07 sept. 2022
2	Cyberattaques : introduction aux techniques générales utilisées.	14 sept. 2022
3	Risques en cybersécurité : Facteurs Technologiques -Configurations, vulnérabilités...etc.	

4	Risques en cybersécurité : facteurs procéduraux -Organisation et gouvernance, meilleurs pratiques, séparation des responsabilités et des pouvoirs.	28 sept. 2022
5	Risques en cybersécurité : facteurs humains -Erreurs et négligences, limitations, manque de formation, biais cognitifs.	05 oct. 2022
6	**Semaine d'études**	12 oct. 2022
7	**Examen Intra**	19 oct. 2022
8	Risques liés aux médias sociaux et santé mentale : phénomènes de bulles, désinformation, cyberintimidation, pédo-piégeage.	26 oct. 2025
9	Profilage des cyberattaquants et des cyber-défenseurs : motivations, comportements.	02 nov. 2022
10	Ingénierie sociale : analyse des mécanismes d'influence et de tromperie,	09 nov. 2022
11	Ingénierie sociale : études de cas, exercices pratiques : planification et exécution d'une attaque reposant sur l'ingénierie sociale.	16 nov. 2022
12	Techniques défensives basées sur l'analyse comportementale (pots de miel, Intelligence artificielle et machine learning… etc).	23 nov. 2022
13	Techniques défensives basées sur la sensibilisation des utilisateurs : utilisation des mots de passes (choix, réutilisation, gestionnaires de mots de passe), utilisation des techniques modernes	30 nov. 2022
14	Etudes des problématiques psychologiques et sociales liées aux mécanismes d'authentification, : choix et réutilisation des mots de passe, acceptabilité sociale de la biométrie, protection de la vie privée	07 déc. 2022
15	**Examen final**	14 déc. 2022

6. Évaluation du cours :

- Examen de mi-session : 30 %
- Examen de fin de session : 35 %
- Devoirs :35 %

Les devoirs seront le fruit du travail personnel de l'étudiant(e). Même si les devoirs doivent répondre à certains critères spécifiques, au moins 25 % de la note pourra être attribuée pour des éléments tels que : qualité de la langue, qualité de la présentation, propreté du travail, utilisation des notions couvertes et expérimentation supplémentaire des logiciels.

Aucun délai pour la remise des travaux ne sera négociable (sauf force majeure) moins de 4 jours avant l'échéance prévue.

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)

La communauté universitaire s'engage à lutter contre les inconduites, le harcèlement et les violences à caractère sexuel. Dénonçons toute forme de violence.

Ensemble, accomplissons un pas de plus en complétant la formation obligatoire en ligne : "La banalisation des violences à caractère sexuel".

uqo.ca/bimi/formation-obligatoire

Pour de plus amples renseignements consultez :

bimi@uqo.ca

UQO
BUREAU D'INTERVENTION EN MATIÈRE D'INCONDUITE

8. Principales références :

NOTES DE COURS : disponibles via Moodle.

Références recommandées pour le cours

Nicolas Arpagian**,** *LA CYBERSÉCURITÉ. ISBN: 978-2-7154-1121-0*

9. Page Web du cours :

https://moodle.uqo.ca