# Faculté des Sciences Appliquées de Béni Mellal
# Avis de soutenance d'une thèse de doctorat

Le Doyen de la Faculté des Sciences Appliquées de Béni Mellal porte à la connaissance du public que **M. Mohamed ZAOUI** soutiendra une thèse de doctorat intitulée : **Advancing Cybersecurity in Morocco: A Human-Centric Approach to Assessing Cybersecurity Awareness and Culture**

La soutenance publique aura lieu le **28 Novembre** 2026 à 14h, au Pôle des Études Doctorales, devant le jury composé de :

| | | | |
|---|---|---|---|
| **Président** | Mohamed Baslam | PES | FST de Béni Mellal, USMS |
| **Rapporteur** | Khalid Zebbara | PES | FSA Ait Melloul, UIZ |
| **Rapporteur** | Guezzaz Azidine | MCH | EST Essaouira , UCA |
| **Rapporteur** | Yousef El Mourabit | MCH | FST de Béni Mellal, USMS |
| **Examinateur** | Abderrazak Farchane | MCH | FSA de Béni Mellal, USMS |
| **Co-directeur de thèse** | Prof. Yassine Sadqi | MCH | FST de Marrakech, UCA |
| **Directeur de thèse** | Prof. Said Safi | PES | FSA de Béni Mellal, USMS |



# Fiche d'informations sur la thèse

**Nom du doctorant :** Mohamed ZAOUI

**Formation doctorale :** Mathématiques et Informatique

**Spécialité :** Informatique et Cybersécurité

**Laboratoire :** Laboratoire d'Innovation en Mathématiques, Applications et Technologies de l'Information (LIMATI)

**Diplômes antérieurs**

Master : Master Informatique des Systèmes Répartis, Faculté des Sciences d'Agadir, affiliée à l'Université Ibn Zohr.

Licence : Licence Professionnelle en Ingénierie Informatique, Faculté des Sciences d'Agadir, affiliée à l'Université Ibn Zohr.

**Directeur de thèse :** Prof. Said SAFI

Faculté des Sciences Appliquées de Béni Mellal, Université Sultan Moulay Slimane.

**Co-directeur de thèse :** Prof. Yassine SADQI

FST de Marrakech, Université Cadi Ayyad.

## Articles publiés

1. **Zaoui, M., Zineddine, A., Sadqi, Y., & Said, S.** (2026). Artificial intelligence in cybersecurity: Addressing ethical considerations and legal implications. EDPACS, 1–8. DOI : 10.1080/07366981.2026.2645143

**2. Zineddine, A., Rehaimi, A., Zaoui, M., Belfaik, Y., Sadqi, Y., & Safi, S.** (2025). LLM-based assessment of HTTPS cybersecurity awareness: Dataset from Moroccan web users and webmasters. Data in Brief, 112024.
DOI : 10.1016/j.dib.2025.112024

**3. Zaoui, M., Zineddine, A., Sadqi, Y., & Safi, S. (2025).** Digital transformation in the Moroccan public sector and cybersecurity challenges. EDPACS, 1–12. DOI : 10.1080/07366981.2025.2543295

**4. Zaoui, M., Yousra, B., Yassine, S., Yassine, M., & Karim, O.** (2024). A comprehensive taxonomy of social engineering attacks and defense mechanisms: toward effective mitigation strategies. IEEE Access, 12, 72224–72241. DOI : 10.1109/ACCESS.2024.3403197

**5. Zaoui, M., & Sadqi, Y. (2025).** The impact of ChatGPT on cybersecurity: Balancing benefits against risks. Recent Advances in Internet of Things Security, pp. 142–152. CRC Press. DOI : 10.1201/9781003587552-16

**6. Zineddine, A., Zaoui, M., Sadqi, Y., & Safi, S. (2025).** Revealing CDN-Side Cybersecurity Risks in HTTPS Connections. Proceedings of I2ASD'25. Springer Nature. DOI : 10.1007/978-3-031-97825-8_83

**7. Zaoui, M., & Sadqi, Y. (2023).** Toward understanding the impact of demographic factors on cybersecurity awareness in the Moroccan context. International Conference on Artificial Intelligence and Green Computing, pp. 207–214. Springer Nature. DOI : 10.1007/978-3-031-46584-0_16

# Résumé

La transformation numérique constitue une priorité pour la modernisation du secteur public marocain. Les institutions publiques, notamment les juridictions, développent des services numériques afin d'améliorer la qualité des prestations et l'efficacité administrative. Cette évolution expose toutefois les informations sensibles et les services publics à de nouveaux risques de cybersécurité.

Les mesures techniques doivent s'accompagner d'une attention aux facteurs humains. La connaissance des menaces, les pratiques de sécurité, les procédures et les conditions organisationnelles influencent la protection des systèmes. Cette thèse étudie ces dimensions à travers une approche centrée sur l'humain, articulant diagnostic de la sensibilisation, analyse de l'ingénierie sociale et développement de la culture de cybersécurité.

La première contribution consiste en une étude de cas quantitative menée auprès du personnel des tribunaux de Guelmim, couvrant la Cour d'appel, le Tribunal de première instance et le Tribunal de la famille. Le questionnaire examine notamment la sécurité des mots de passe, l'ingénierie sociale, les pratiques numériques, la formation et la connaissance de la législation pertinente. Les 113 réponses recueillies sur un effectif de 122 personnes permettent de dresser un diagnostic local des indicateurs de sensibilisation et des pratiques déclarées.

Les résultats mettent en évidence des lacunes qui motivent des actions de sensibilisation et un examen des conditions institutionnelles de sécurité. Ils décrivent le terrain étudié et ne constituent pas une mesure exhaustive de la culture organisationnelle ni une estimation représentative de l'ensemble du secteur public marocain.

# Résumé suite

La deuxième contribution propose une taxonomie structurée des attaques d'ingénierie sociale et des mécanismes de défense. Fondée sur une synthèse de la littérature, elle organise les caractéristiques des attaques ainsi que les contre-mesures techniques et non techniques. Elle fournit un support d'analyse pour comprendre les menaces et identifier des réponses adaptées au contexte.

La troisième contribution développe un cadre conceptuel de culture de cybersécurité fondé sur les cinq P : Prérequis, Personnes, Processus et Politiques, Performance et Perception. Le cadre organise dix-sept facteurs issus de la littérature et propose sept étapes de mise en œuvre. Il souligne le rôle continu de la direction et relie les dimensions humaines aux pratiques organisationnelles de sécurité.

La thèse articule ainsi trois objectifs : diagnostiquer les lacunes de sensibilisation, comprendre les mécanismes des attaques et construire les conditions favorables à une culture de cybersécurité. Elle propose des pistes aux décideurs publics et aux professionnels pour orienter les actions de formation, les procédures et l'évaluation des pratiques. L'efficacité du cadre en situation réelle reste à examiner par une évaluation auprès de praticiens et des expérimentations organisationnelles.

Mots-clés : Cybersécurité ; sensibilisation à la cybersécurité ; culture de cybersécurité ; facteurs humains ; ingénierie sociale ; taxonomie ; mécanismes de défense ; cinq P ; transformation numérique ; secteur public marocain.