Cybersecurity Projects 2026-27

Contents

Adaptive and Inclusive Cybersecurity Education

Supervisor: Tasmina Islam

Areas: Artificial Intelligence, Machine learning / Deep learning, Cybersecurity, Human-centred computing (human-computer interaction), Natural Language Processing

(Back to Scholarship Not Allocated)

Project Description

Cybersecurity awareness is essential in a digital society, yet current initiatives are often generic and fail to address the needs of underrepresented groups such as children, minority communities, and people with disabilities. This project proposes to design adaptive awareness environments that apply artificial intelligence to deliver personalised, culturally relevant, and accessible cybersecurity training.

Participants will engage with interactive simulations of cyber threats (e.g., phishing, ransomware, data leakage) enhanced by generative AI, which can create customised attack narratives and provide context-aware, real-time feedback. Alongside the development of adaptive systems, the project will employ interviews and focus groups, combined with behavioural analytics and surveys, to understand user needs, evaluate effectiveness, and identify different types of cybersecurity users (e.g., risk-takers, cautious users, or overconfident participants). It will also explore new ways of measuring awareness outcomes, introducing resilience-based metrics such as detection speed, recovery performance, and transfer of skills across scenarios.

By combining technical innovation with human-centred research, this work seeks to establish a scalable framework for evidence-driven cybersecurity awareness, empowering diverse populations to navigate digital risks safely. Prospective students can discuss options with the supervisor.

References

1. Segupta, S., Varma, U., & Islam, T. (2025). Empowering Cybersecurity Education: A Review of Adaptive Learning Paradigms and Practical Implications. In Joint Proceedings of IS-EUD 2025: 10th International Symposium on End-User Development, 16-18 June 2025, Munich, Germany.: 3rd International Workshop on Cyber Security Education for Industry and Academia.
2. Hedges, M., & Islam, T. (2024). VirSec - Immersive Security Training within Virtual Reality. In 17th International Conference on Advanced Visual Interfaces: 2nd International Workshop on CyberSecurity Education for Industry and Academia (CSE4IA 2024)
3. Islam, T & Zou, Y 2023, ChildSecurity: A Web-based Game to Raise Awareness of Cybersecurity and Privacy in Children. in Cybersecurity Challenges in the Age of AI,Space Communications and Cyborgs.

Designing for user-to-user consent and safety in online platforms

Supervisor: Kovila Coopamootoo

Areas: Cybersecurity, Human-centred computing (human-computer interaction)

(Back to Scholarship Not Allocated)

Project Description

The practice of sharing private, sensitive or intimate content is prevalent online and is digitally-mediated by online platforms such as dating apps, messaging or communication platforms, or online social networks. However, users of such platforms are mostly left to manage the risks associated with un-consensual behaviours, such as further content distribution, manipulation, storage or unsolicited exchange, on their own. Such risks include privacy violations, broken interpersonal trust, or online harms, such as extortion, image-based sexual abuse, as well as reputation damage and associated social harms.

While the UK's Online Safety Act 2023 has established offences for the un-consensual exchange of intimate content, there is still a lack of platform design supporting (1) consent conversations, specifications and the enforcing of boundaries; and (2) what happens when users change their mind or relationships break down and wish to modify or revoke consent.

This PhD project will investigate users' consent needs in online platforms, and design and evaluate consent mechanisms for user-to-user consent. The project is the intersection of privacy / security and human-computer interaction, and potentially AI.

References

- Geeng, C. et al., 2020. Usable sexurity: Studying People's concerns and strategies when sexting.
https://www.usenix.org/conference/soups2020/presentation/geeng
- Qin, L. et al., 2024. "Did they consent to that?": Safer digital intimacy via proactive protection against image-based sexual abuse.
https://arxiv.org/html/2403.04659v1
- Qin et al., 2023. Towards safer intimate futures: recommendations for tech platforms to reduce image based sexual abuse.
https://www.eswalliance.org/toward_safer_intimate_futures_recommendations_tech_platforms_reduce_image_based_abuse
- Im et al., 2024. Yes: Affirmative consent as a theoretical framework for understanding and imagining social platforms.
https://dl.acm.org/doi/abs/10.1145/3411764.3445778

Validation of Cyber Threat Intelligence Leveraging Large Language Models

Supervisor: Hannah Cao

Areas: Cybersecurity

(Back to Scholarship Not Allocated)

Project Description

Cyber Threat Intelligence (CTI) is central to modern cybersecurity, equipping organisations to anticipate and mitigate evolving threats. Effective CTI enables proactive defence through timely incident response, patch management, and vulnerability awareness. However, the rapid advancement of Artificial Intelligence (AI), particularly Large Language Models (LLMs), has introduced new challenges. While LLMs offer powerful tools for processing the unstructured data that dominates CTI, they can also be exploited by malicious actors to generate fabricated intelligence at scale. Such disinformation threatens to mislead analysts, poison datasets, and erode the trust essential for collaborative defence.

Existing validation methods, which rely heavily on structured Indicators of Compromise (IoCs) or source reputation, are ill-equipped to handle nuanced, text-based intelligence of uncertain authenticity. This project addresses this critical gap by developing scalable methods to detect fabricated CTI. Specifically, it proposes leveraging LLMs themselves, guided by structured analysis and corroboration against external sources, to assess the likelihood of falsehood in unstructured reports.

The research will deliver a robust framework for validating CTI, strengthening resilience against AI-driven disinformation campaigns. By enhancing confidence in intelligence sharing, the project aims to reduce the risks of misallocated resources and flawed security postures, ultimately supporting more effective cybersecurity practices. Beyond technical validation, the project will also provide an educational platform for cybersecurity practitioners, equipping them with the knowledge and tools to recognise and counteract fabricated CTI in practice.

Scaffolding Student Learning through GenAI in Cybersecurity Education

Supervisor: Hannah Cao / Ievgeniia Kuzminykh

Areas: Artificial Intelligence, Cybersecurity, Education

(Back to Scholarship Not Allocated)

Project Description

Scaffolding, a concept rooted in Vygotsky's Zone of Proximal Development (ZPD), refers to the instructional supports that help learners bridge the gap between their current abilities and learning goals. Traditionally, scaffolding has been provided by tutors, peers, or carefully designed instructional materials.

Generative AI (GenAI) tools such as ChatGPT are now transforming higher education. With the capacity to generate coherent text, explain complex concepts, and solve problems, these tools offer new opportunities for personalised learning. However, their adoption remains controversial. While they can enrich teaching and learning, concerns persist regarding academic integrity and the risk that students may bypass deeper cognitive engagement.

This project responds to these challenges by designing and evaluating a GenAI-driven scaffolding system for cybersecurity education. Rather than supplying direct answers, the system will prompt reflection, break down problems into manageable steps, and encourage exploration, drawing on established pedagogical approaches such as inquiry-based learning. By integrating advances in AI with the principles of effective scaffolding, this project aims to enhance cybersecurity education while contributing to broader debates about the ethical and pedagogical role of AI in higher education.