MODULE DESCRIPTOR

Module Title

Social & Human Factors In Cyber Security

Reference	CM2133	Version	1
Created	November 2023	SCQF Level	SCQF 8
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

This module aims to equip students with an understanding of human factors in cybersecurity, fostering the development of skills in strategic risk management, the design of usable security measures, and effective stakeholder engagement. This preparation enables students to promote security awareness and provide informed recommendations for addressing social and human factor challenges.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Distinguishes the significance of human factors in cybersecurity via key behaviours impacting security.
2	Practice usability inspection, inquiry, and evaluation techniques to analyse user behaviour and perceptions within security mechanisms.
3	Undertake an exploration and examination of materials and real-world situations related to social and human factor issues linked to Cyber Security.
4	Show an awareness of guidance and recommendations to enhance stakeholders' security awareness in addressing social and human factor issues related to Cyber Security.

Indicative Module Content

Human-centred security: Usability Inspection, Enquiry and Evaluation; Usable Security and Trade-offs; User Research, Personas, and Design for Human Values; Behaviour Change Approaches and Frameworks; Nudging and Persuasion for Cybersecurity; HCI design processes, standards and guidelines. Human Capabilities and Limitations: Memory, Biases and strategies, Error, violations and mitigations; Risk perception and Trust; Alarm Fatigue, One-Time Passwords and best practices; Models and measurements of situational awareness; Task Allocation, Error Mitigation. Stakeholder Engagement and Assessment Criteria: socio-technical case study analysis; Awareness, Education, and Positive Security; Ethical Considerations; Environmental factors; Employee and Developer Perspectives.

Module Ref:	CM2133 v1

Module Delivery

Lectures introduce and illustrate key concepts, while practical skills are honed through a series of laboratory exercises.

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	A written coursework to assess the understanding of social and human factor issues related to Cyber Security for a selected case study.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CM2133 v1

INDICATIVE BIBLIOGRAPHY

1	Corradini, I. (2020).?Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology?(Vol. 284). Springer Nature.
2	Leukfeldt, R., & Holt, T. J. (2020). The Human Factor of Cybercrime. Routeledge.
3	Zinatullin, L. (2016).?The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour. IT Governance Ltd.
4	Tavani, H. T. (2016).?Ethics and technology: Controversies, questions, and strategies for ethical computing. John Wiley & Sons.
5	Tryfonas, T. (Ed.). (2017). Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings?(Vol. 10292). Springer.