MODULE DESCRIPTOR

Module Title

Human Factors in Security

Reference	CMM542	Version	2
Created	February 2024	SCQF Level	SCQF 11
Approved	January 2023	SCQF Points	15
Amended	April 2024	ECTS Points	7.5

Aims of Module

To enable students to critically appraise the role of human factors in cyber security; particularly when designing secure and usable systems, considering key aspects including security, privacy, usability, technology acceptance, and the socio-technical context.

Learning Outcomes for Module

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

1	Evaluate the role of human behaviour in security.
2	Appraise the usability criteria of security mechanisms.
3	Synthesise techniques from interaction design, software engineering, and security engineering to design secure systems.
4	Appraise measures that an organisation requires to ensure long-term, productive security.

Indicative Module Content

The role of human factors and Positive Security; Behavioural Aspects and Acceptance for Designing Secure and Usable Systems; Human error; Security and Privacy Requirements Engineering; Usable, Security Design Techniques and Processes; Requirements and Threats/Attacks Modelling; and Security architecture; Usable Authentication; Usable Authorization; Security awareness, education, and training; Security economics and entrepreneurship.

Module Delivery

Key concepts are introduced and illustrated through lectures and directed reading. The understanding of students is tested and further enhanced through lab and tutorial sessions.

Module Ref:	CMM542 v2

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	40
Non-Contact Hours	120	110
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
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:	This is a coursework where students will appraise all the relevant human factors in designing usable security for a given scenario.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade D is required to pass the 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.

INDICATIVE BIBLIOGRAPHY

1. FAILY, S. 2018. Designing Usable and Secure Software with IRIS and CAIRIS. Springer.
2. FERNANDEZ, E. B. 2013. Security Patterns in Practice: Designing Secure Architectures Using Security Patterns. Wiley.
3. CRANOR, L. F. and GARINKEL, S. 2005. Security and Usability: Designing Secure Systems that People Can Use. O?Reilly.
4. Symposia on Usable Privacy and Security. 2015-2021. https://www.usenix.org/conferences/byname/884
5. GARFINKEL, S., and LIPFORD, H. R. 2014. Usable Security: History, Themes, and Challenges. Synthesis Lectures on Information Security, Privacy, and Trust. Morgan & Claypool.
6. ROPER, C. A., GRAU, J. J., and FISCHER, L. F. 2006. Security education, awareness, and training: from theory to practice. Elsevier Butterworth-Heinemann.
7. BREAUX., T., ed., 2020. An Introduction to Privacy for Technology Professionals. 2020. IAPP Publication.
8. ANDERSON, R., 2020. Security Engineering. Wiley