WM9PB-15 Human Factors

24/25

Department
WMG
Level
Taught Postgraduate Level
Module leader
Elzbieta Titis
Credit value
15
Module duration
4 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module focuses on human factors (HFs) in cyber security by investigating a range of factors (individual, organisational, societal, and technological) to show how HFs vulnerabilities may impact on cyber security risks.

Adopting a technology-centric viewpoint in which users' cognitive characteristics, needs and motivations are ignored has proved times and again to be insufficient. Moreover, cyber security culture does not always translate to rules compliance behaviour. Conflicts among cyber security rules and procedures may also trigger human vulnerabilities. An inclusive, multidisciplinary, and holistic approach is needed instead to address these vulnerabilities and the reason behind incorrect security actions, including both errors and violations, to support organisations in becoming more effective against cyber-attacks and threats.

In this module you will learn about a range of human characteristics (physical, cognitive, social and emotional) as they relate to the strengths and limitations of humans, and how these can introduce errors into cyber security resulting in a successful cyber attack or data breach; aspects of the broader context in which interaction with security takes place, including organisational and societal perspectives on security, will be also covered. Moreover, as the interaction between the human and the system influences human performance relevant to cyber security, you will also learn to evaluate the principal features of HFs in current and planned online secure systems to design security that is usable and acceptable to a range of human actors (e.g., end-users,

administrators, and developers) by engaging stakeholders and negotiating security solutions that meet their needs.

As a result, you will acquire knowledge and skills increasingly desirable in industry to address HFs in cyber security by adopting a user-centred perspective for incorporating non-technical countermeasures (such as user awareness) to manage and support cyber security in organisations.

Module aims

This module aims to provide the students with a critical awareness of HFs in cyber security and allow them to apply advanced technical concepts and practices for managing HFs in organisations using a psychological perspective.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The syllabus will include (but is not limited to):

- Cognitive ergonomics.
- Usable security.
- Cognitive hacking.
- Persuasion and social influence.
- Behaviour change.

Learning outcomes

By the end of the module, students should be able to:

- Critically understand key aspects of HFs and demonstrate critical awareness of HFs research and theory in cyber security, including current problems and psychological perspective.
- Implement methodologies appropriate for solving complex problems in HFs, demonstrating self-direction and originality.
- Report and critically debate the outcomes of investigations, followed by proposing new avenues for research.
- Research and analyse real-world situations that relate to HFs in cyber security, making informed inferences to relevant theory and empirical scholarship.
- Provide advice and recommendations about how to tackle HFs issues in cyber security, integrating scholarship and making theory useful for implementing evidence based practice.

Indicative reading list

Rogers et al. (2007). Interaction Design: Beyond Human-Computer Interaction. Forth Edition. John Wiley and Sons.
Corradini (2020). Building a cybersecurity culture in organizations. How to Bridge the Gap

Between People and Digital Technology (Vol. 284). Berlin/Heidelberg, Germany: Springer International Publishing.
Thaler and Sunstein (2009). Nudge: Improving decisions about health, wealth, and happiness. Penguin Books Ltd.

View reading list on Talis Aspire

Research element

- Redesigning a system for better usability.
- Evaluating usability of a system for minimising human error.
- Evaluating principles of persuasion in social engineering for stronger cognitive resilience.
- Designing behaviour change intervention for stronger cyber security.

Interdisciplinary

The module uses insights from Psychology, Sociology and Criminology to understand usability issues, human behaviour, adversarial behaviour, requirements gathering and innovation processes relevant for cyber security.

Subject specific skills

Designing and evaluating usable systems as they pertain to cyber security.
Applying different disciplinary perspectives to solve design and deployment challenges, and to plan for HFs in organisations, including behaviour change interventions.
Locating, summarising and critically evaluating examples of recent controversy and progress in HFs.

Transferable skills

Researching literature.
Communication, critical thinking, and problem solving.
Time management.
Teamwork.
Competence in multi-disciplinary research.
Presenting to peers a critical evaluation of own research work.
Defending own work to an audience of peers.

Study

Study time

Type	Required
Lectures	7 sessions of 1 hour (5%)
Practical classes	23 sessions of 1 hour (15%)
Online learning (independent)	15 sessions of 1 hour (10%)
Private study	45 hours (30%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Independent activity between labs/workshops, following up on activities initiated in previous labs/workshops or preparing for upcoming labs/workshops.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Assessment component			
Written asynchronous portfolio	80%	50 hours	Yes (extension)

The portfolio will include a selection of different written tasks: a) commentary on critical HFs in cyber security using case study approach; b) a short report on usability/security trade-offs either compiling a catalogue of patterns addressing different instances of the conflict between security and usability OR analysing a case study using a metrics based-model; c) a proposal of behaviour change intervention OR social engineering awareness material; and d) a thematic reflection on a written text, which can be an article, essay, or book. All the written tasks to be submitted as a single submission at one point in time.

Reassessment component is the same

Assessment component

	Weighting	Study time	Eligible for self-certification
Blog/presentation on how to tackle HFs issues in cyber security	20%	10 hours	No

Students will create a Weakest Link in Cyber Security Resource as a group. The blog will be approximately 800 words including content informed by science and based on research evidence. Students will then deliver group presentations to the class in the scheduled class time, talking about one issue from the blog.

Reassessment component is the same

Feedback on assessment

Written feedback for each assignment.
Verbal feedback during tutorial sessions.
Summative feedback on assignments.

Availability

There is currently no information about the courses for which this module is core or optional.