

WM241-18 Human Behavior in Cyber Systems

24/25

Department

WMG

Level

Undergraduate Level 2

Module leader

Elzbieta Titis

Credit value

18

Module duration

30 weeks

Assessment

100% coursework

Study location

University of Warwick main campus, Coventry

Description

Introductory description

Human-computer interaction (HCI) is concerned with designing interactions between human activities and the computational systems that support them, and with constructing interfaces to afford those interactions. Interaction between users and computational artefacts occurs at an interface that includes both software and hardware. Human behaviour should influence interface design and implementation of core functionality. For end-users, the interface is the system, meaning design in this domain must be interaction-focused and human-centred. It is therefore imperative that during the design phase of this human-computer interface cyber security component of human behaviour is addressed. One of the most significant challenges in the cyber domain is the transfer of meaning between the fully human agent, and the fully digital sub-system. Failure to correctly align human behaviour with computing sub-system behaviour has contributed to numerous, historic cyber security problems.

In addition, psychological traits and individual differences among computer system users can further explain vulnerabilities to cyber security attacks and crimes, as cognitive biases and impaired brain health can make individuals more susceptible to exploitation by cyber criminals. Cyber security procedures and policies are prevalent countermeasures for protecting organizations from cybercrimes and security incidents, however, without considering human

behaviours, implementing these countermeasures will remain useless.

Consequently, this module places the person at the centre of the cyber domain by addressing the problematic of human factors in general and usable security in particular. As such, the focus is on trade-offs between usability and security on the one hand, and human psychology and human error on the other hand. Human vulnerabilities will be addressed in detail to build greater cyber resilience, and narrative around security awareness/training programmes and security culture will be also introduced for understanding broader, non-technical influences on security through minimising human related risks.

Module aims

1. To provide students with high levels of skills, knowledge, and competency around human factors (HFs) and human-computer interaction (HCI) research.
2. To provide students with the opportunity to contextualise and apply learning in the field of HCI by undertaking an independent usability assessment of an online system to address trade-offs with security using appropriate methodological and analytical techniques.
3. To provide students with in-depth knowledge of human psychology and human error to understand human traits and behaviours commonly exploited by malevolent actors.

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 content of this module will be taught from a cyber security perspective, embracing cognitive science and human factors engineering, and will include:

- Foundations;
- User-centred design and testing;
- Usable security incl. trade-offs;
- Human factors and security.

Specifically, the module will cover:

- Cognitive hacking, incl. psychological levers used by cyber criminals;
- Human error and insider threat;
- Approaches and frameworks for changing behaviour;
- Approaches and frameworks for ethical decision making;
- Nudging and persuasion towards better cyber security;
- Human cognitive capabilities and limitations;
- Cyber security culture and hygiene.

As such the module is highly interdisciplinary, incorporating diverse concepts and approaches from many different disciplines, including computer science, psychology, ethics and cyber security.

Learning outcomes

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

- Select and critically evaluate the different factors that are pertinent to the security and usability of secure systems in their contexts of use.
- Apply techniques from interaction design to design and evaluate secure systems including security concerns for web application security.
- Analyse the relationship between user behaviour in digital space and cyber security consequences.
- Propose a theory-informed intervention appraising the role of human factors in delivering cyber security.

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](#)

Interdisciplinary

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

Subject specific skills

Knowledge of issues and problems in HCI.

Understanding of different disciplinary perspectives and ability to apply them to solve design and deployment challenges pertaining to cyber security.

Devising, planning, and executing requirements investigations and system evaluation, and presenting findings in a clear and effective manner.

Demonstrating awareness of current areas of research in human factors by locating and summarising examples of recent controversy and progress.

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 their own work to an audience of peers.

Study

Study time

Type	Required
Lectures	18 sessions of 1 hour (10%)
Supervised practical classes	18 sessions of 1 hour (10%)
Online learning (independent)	15 sessions of 1 hour (8%)
Private study	57 hours (32%)
Assessment	72 hours (40%)
Total	180 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 A4

	Weighting	Study time
Security and usability trade-offs	30%	20 hours
In this coursework, students will be asked to analyse the security and usability of a system based on a security-usability threat model.		
Written asynchronous portfolio	70%	52 hours
The portfolio will include a selection of different written tasks: a) proposal of improved usability design for a system; b) experiential reflection on practical lab tasks with evidence of completing tasks*; c) research paper selection incl. textual reflection**; d) short critical reflection on a given statement; and e) proposal of behaviour change intervention for a given scenario. *With the experiential reflective piece, students will analyse their own personal learning experience answering the following questions: How has the material affected me? What have I learned? How does the material catch my attention? Are there unsolved questions or critical issues? How will the material affect my future thinking? **With the textual reflective piece, students will analyse a		

Weighting

Study time

written text, which can be an article, essay or book chapter to then formulate their opinion, analysis and interpretation of the material backed up using specific quotations. All the written tasks to be submitted as a single submission at one point in time.

Feedback on assessment

Written feedback for each assignment.

Verbal feedback during tutorial sessions.

Summative feedback on assignments.

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
 - Year 2 of H651 Cyber Security
 - Year 2 of H651 Cyber Security
 - Year 2 of H651 Cyber Security