JÖNKÖPING UNIVERSITY
School of Engineering

COURSE SYLLABUS

Human Aspects of Cybersecurity, 7.5 credits

Mänskliga aspekter av cybersäkerhet, 7.5 högskolepoäng

Course Code:	T2MAAC	Education Cycle:	Second-cycle level
Confirmed:	Sep 01, 2025	Disciplinary domain:	Technology
Valid From:	Aug 31, 2026	Subject group:	Computer Technology
		Specialised in:	A1N Second cycle, has only first-cycle course/s as entry requirements
		Main field of study:	Computer Science

Intended Learning Outcomes (ILO)

On completion of the course the student shall:

Knowledge and understanding

- display knowledge of how cybersecurity behavior is impacted by the social environment, personal traits and cognitive abilities
- display knowledge of different models that explain how cybersecurity behavior is formed
- display knowledge about personal traits and motivations driving cybercriminals

Skills and abilities

- demonstrate skills in applying human-centered design methods within cybersecurity
- demonstrate skills in applying models to explain and predict behavior in cybersecurity contexts

Judgement and approach

- demonstrate insight into the interplay between security and usability
- demonstrate an insight into the societal, legal, and ethical aspects of human aspects of cybersecurity

Content

Cybersecurity is often treated as a purely technical topic, even though most incidents are made possible by human mistakes or attackers who exploit human nature. Cybersecurity is a socio-technical phenomenon resulting from the interplay between technology, humans and the social environment where this interplay takes place. This course focuses on the human aspects of cybersecurity and begins with an exploration of what we expect users to do to comply with cybersecurity requirements. Then, humans' ability to comply with those requirements is explored by discussing how the social environment, personal traits and cognitive abilities shape cybersecurity behaviour. The students are also introduced to models that explain different aspects of how cybersecurity behaviour is formed. During the course, the students will be introduced to human-centred design methods and learn how to apply those to assess and evaluate cybersecurity concepts, solutions, and systems.

The course includes the following elements:

- Exploration of models that are commonly used to explain cybersecurity behaviour, (e.g., FOGG and Protection Motivation Theory)
- Human-centered design methods, such as the double diamond process
- Exploration of the usable security paradigm

Type of instruction

The course consists of lectures and project work.

Language of instruction is in English.

Entry requirements

The applicant must hold a minimum of a bachelor's degree (i.e., the equivalent of 180 ECTS credits at an accredited university) with at least 90 credits in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent. Proof of English proficiency is required.

Examination and grades

The course is graded 5, 4, 3 or U.

Registration of examination:

Name of the Test	Value	Grading
Project	7.5 credits	5/4/3/U

Course literature

Please note that changes may be made to the reading list up until eight weeks before the start of the course.

M. Angela Sasse and Awais Rashid, The Cyber Security Body of Knowledge v1.1.0, 2021,Human Factors, University of Bristol, https://www.cybok.org/knowledgebase1_1/