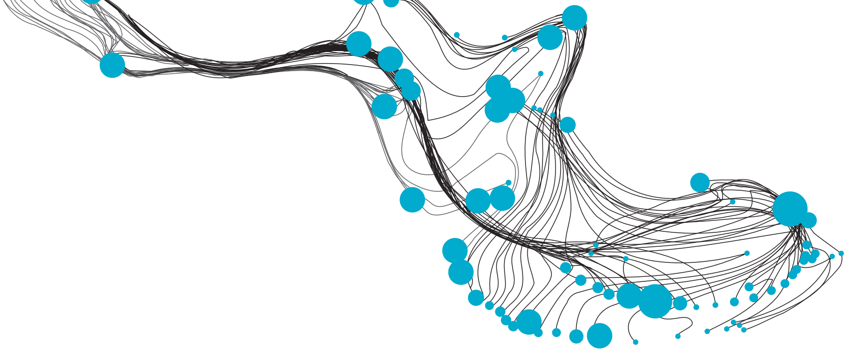
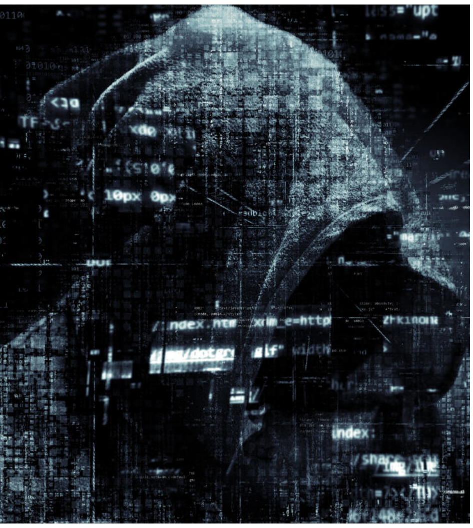


WWW.UTWENTE.NL/MAJORMINOR

MINOR
CYBERSECURITY & CYBERCRIME



CYBERSECURITY AND CYBERCRIME GO HAND IN HAND AS TWO FACES OF THE SAME COIN. WHILE THE INTERNET IS ONE OF THE GREATEST ACHIEVEMENTS OF HUMANITY, IT IS ALSO A GREAT ENABLER FOR MALICIOUS ACTIVITIES. BUT HOW DOES THIS AFFECT US IN PRACTICE? WHAT ATTACKS CAN WE SUFFER? WHAT CONSTITUTES CYBERCRIME? AND HOW DO WE IDENTIFY IT AND FIGHT IT? ARE WE, AS INDIVIDUALS, ORGANIZATIONS AND SOCIETY AT LARGE, READY FOR IT?

WHAT IS A HTHT MINOR?

A HTHT-minor fits within the UT profile: High Tech, Human Touch. The minor is offered in English and accessible for both national and international students. The goal of the HTHT-minor is to illuminate specific societal themes for which the UT develops High Tech Human Touch solutions. These solutions are created by conducting high-quality research. Both the form and the content of the minors are High Tech Human Touch (multidisciplinary) and are profiling for the student.

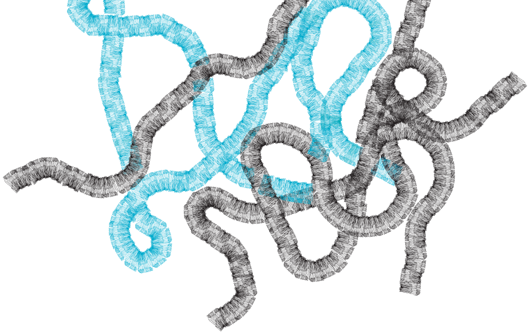
The UT offers most HTHT-minors in a coherent package of 2 (30 EC). There are also HTHT minors of 15 EC that do not belong to a package. You can choose one of these minors and combine this with one minor of a package. If possible, you can even choose 2 minors from different packages.

MINOR INFORMATION

The Internet has started out as a toy academic exercise, but by now it is one of the greatest technological achievements of humanity. The Internet has changed the way we interact with the world around us, but it has also paved the way for new forms of crime.

This minor will introduce you to the fields of Cybersecurity and Cybercrime. Cybersecurity encompasses measures taken to protect a computer system, a network, or the Internet as a whole, against unauthorized access or attack. As far as the Internet is concerned, however, the spectrum of abuse is large: it ranges from cyberdeviance (a behavior outside or at the edge of the formal norms of society, but not yet illegal) to real cybercrime (an activity that violates a set of legal norms). And yet, between these extreme examples, our psychological, regulatory and ethical frameworks are still catching up with the advancements in technology and technological crime.

UNIVERSITY OF TWENTE.



"I've spent my life defending the Net, and I do feel that if we don't fight online crime, we are running a risk of losing it all."
Mikko Hypponen

The Cybersecurity and Cybercrime minor is a multidisciplinary minor that will cover both high-tech and human-touch aspects of this discipline, and combines them in a hands-on final project. The minor aims at providing a comprehensive, multi-faceted view of the interaction between Internet technology and crime.

Module parts

Project: In the project you will try your hand at a real-life Cybersecurity and Cybercrime event. You will learn to design, implement and document your own Cybersecurity and Cybercrime experiment, with the goal of preventing, investigating or raising awareness about cybercrime.

Internet Technology: You will learn about the basic concepts of the Internet, such as how networks and core Internet services like the Domain Name System work. You will then learn how these concepts are related to common types of Internet attacks, such as scans, worms and Denial of Service attacks.

Digital Forensics for Cybercrime: What needs to be done when we become victim of an attack is still an open question. You will learn how to collect relevant data, how to extract information relevant to a specific attack, how this data can be analyzed and finally how evidence of an attack can be reported.

Privacy and Information Security: Privacy and Information Security are two separate, but inextricably linked topics. You will learn about fair collection of sensitive data on private individuals (privacy), and about protecting the information managed by an organization against unauthorized access (information security)

Governance & Regulation of Cybersecurity: As a transnational phenomenon, cybersecurity cannot be regulated by individual states. You will investigate the differences across countries and organizations and identify and analyze the challenges introduced by such differences. You will then explore how the involvement of governmental as well as non-governmental rule-makers at the national, EU and global level results in new governance challenges.

Psychological aspects of cybercrime: The human side of cybersecurity has many facets. You will learn about crime, as a result of human nature and human development (the person approach to crime), and also as affected by the context of crime (crime science). You will then investigate the topics of social engineering, or "the art of hacking the human", and compliance and fraud in organizations.

Economical aspects of cybercrime: Organizations need to invest in cybersecurity to protect themselves from cybercrime, but are they really ready for when an attack strikes? You will learn how to evaluate the present cybersecurity readiness of an organization and estimating the net economic impact of a cyber attack.

Vulnerability Disclosure and Ethics:. Attackers constantly look for new vulnerabilities to hack systems, while security experts need the same knowledge to secure those systems. You will learn to critically discuss the issue of vulnerabilities in an ethical context, the legal/ illegal status of working with (undisclosed) vulnerabilities, and guidelines about vulnerability disclosure.

MORE INFORMATION

Minorcoördinator:
Anna Sperotto
Zilverling Zi-5098
T: 053 489 2812
E: a.sperotto@utwente.nl

For the 2021 Edition of the Minor
please contact both:
-Anna Sperotto - a.sperotto@utwente.nl
-Roland van Rijswijk-Deij -
r.m.vanrijswijk@utwente.nl

For more information about this minor and for general information about minors:
www.utwente.nl/majorminor/