



E4J UNIVERSITY MODULE SERIES

# CYBERCRIME

UNODC's Education for Justice (E4J) initiative, a component of the Global Programme for the Implementation of the Doha Declaration, seeks to prevent crime and promote a culture of lawfulness through educational activities designed for primary, secondary and tertiary levels. These activities will help educators teach the next generation to better understand and address problems that can undermine the rule of law. At the university level, E4J supports academics to teach in UNODC-mandated areas. The areas addressed in the University Modules range from crime prevention and criminal justice, smuggling of migrants and trafficking in persons, organized crime, cybercrime, wildlife crime, anti-corruption, firearms, counter-terrorism to ethics and integrity. The modules are designed for lecturers to adapt and integrate into their courses.



The Doha Declaration:  
**PROMOTING A CULTURE  
OF LAWFULNESS**



High levels of digitalization and digital inter-connectivity have made the world increasingly more complex. Unfortunately, in this complexity cybercriminal activities have also grown exponentially. Whether you are a small business, a fortune 500 company, buying your first smartphone or becoming a cybersecurity expert, you need to be aware of cybercrime. To address this challenge, there is an urgent need for more robust education regarding cybercrime. The E4J initiative's response to this issue has been the development of several educational tools addressing cybercrime, including the University Module Series on Cybercrime. This series is multi-disciplinary in nature and provides resources on different aspects of cybercrime and cybercrime investigation:

- Introduction to cybercrime
- General types of cybercrime
- Legal frameworks and human rights
- Introduction to digital forensics
- Cybercrime investigation
- Digital forensics and technical cybercrime investigations
- International cooperation against cybercrime
- Cybersecurity and cybercrime prevention: strategies, policies and programmes
- Cybersecurity and cybercrime prevention: practical applications and measures
- Privacy and data protection
- Cyber-enabled intellectual property crime
- Interpersonal cybercrime
- Cyber organized crime
- Hacktivism, terrorism, espionage, disinformation campaigns and warfare in cyberspace

The E4J University Module Series on Cybercrime carefully integrates resources collected from around the world related to cybercrime, legislation, investigation and prevention. While the modules provide lecturers with the guidelines and resources to build comprehensive, cross-discipline courses on cybercrime, the corresponding Teaching Guide offers pedagogical guidance for lecturers. These tools are the result of a collaborative effort among leading experts and academics from over 25 countries in 6 different continents.

We envision an educator using these modules to construct a course that best fits the needs of his or her students. Each module is as self-contained as possible, while fitting into an overarching theme. In this sense, the modules can either be selectively used within an educator's existing course or the modules can be used together to create an entire semester course. Educators are encouraged to use various modules from all available E4J University Module Series to create a custom course that meets their individual teaching goals.

---

[unodc.org/e4j](https://unodc.org/e4j)

---



---

@DohaDeclaration

---