
***'On average, Europe faces 4,000 ransomware attacks a day, while cybercrime cost consumers 172 billion dollars last year. In 2016, European citizens were affected by 2 billion data breaches.'***

European Commissioner Julian King, Security Union, 18 April 2018

## Online Module: Executive Summary

Cybercrime is crime that is committed using a computer and a network.

Today our societies depend heavily on digital networks and information systems, and we connect to the internet through many different types of device, from desktop and laptop computers to smartphones and other smart devices. With this digitisation has come the development of criminal activity, both traditional forms that have moved online ('cyber-enabled crime') and new forms that seek to exploit the information systems and their contents.

Cybercrime therefore includes a wide spectrum of offences. These include:

- Attacks against information systems, such as hacking, data theft and website defacement, and a range of network attacks, such as ransomware attacks, spreading malicious code and distributed denial of service (DDoS) attacks;
- Financial cybercrime – large-scale fraud can be committed online via means such as identity theft, phishing, skimming and card-not-present fraud;
- Illegal online content, including child sexual abuse material, incitement to racial hatred and the glorification of violence.

The module targets all law enforcement officers, prosecutors and judges who deal with or in the future may deal with cybercrime and cyber-enabled crime. It aims to introduce the main aspects of these crimes, including identifying and preventing them, and conducting first response and investigation.

The module consists of an introduction, nine topic chapters and a glossary of cybercrime-related terms and abbreviations. In the My Progress section, users can assess their levels of understanding of each of the topics by considering a selection of questions and true/false statements.

The topic chapters are:

1. **Introduction**
2. **Types of Cybercrime and Cyber-Enabled Crime:** This chapter provides an overview of the different types of cybercrimes that law enforcement may face in their investigations.
3. **First Response:** This chapter covers the procedures that should be followed by first responders to incidents of cybercrime and cyber-enabled crime. It includes the preserving and investigating of the crime scene, and the collecting and transporting of devices.
4. **Investigating Cybercrime:** The subject of this chapter is the collecting of information (intelligence and evidence) during an investigation. It does not include digital forensics or e-evidence, which are both covered in Chapter 5.
5. **Digital Forensics and E-Evidence:** This chapter discusses what e-evidence (digital evidence) is, and the objectives and processes involved in digital forensics (the analysis of electronic devices).
6. **Legislation:** In this chapter, the national, regional and international legislation related to cybercrime are presented. It includes the trends of the law-making process and the challenges faced by the judicial authorities.
7. **International Cooperation 1** – **Law Enforcement Cooperation:** The first of two chapters on international cooperation, this chapter addresses the cooperation facilitated by EU and international law enforcement organisations and networks.
8. **International Cooperation 2** – **Judicial and Public Sector Cooperation:** This is the second chapter on international cooperation, and it covers the organisations and networks involved in judicial cooperation and cooperation with the private sector.
9. **Prevention and Capacity Building:** This chapter covers prevention, making people more aware of cybercrime phenomena and of how to avoid becoming victims of cybercrime. It also discusses capacity building, including the education and training of law enforcement personnel, and the resources available to them, to help them tackle cybercrime.
10. **Challenges and Future Trends:** This last chapter of the module presents the cybercrime-related challenges to law enforcement that have arisen in recent years. It also takes a look at the current and likely future trends in the area.