

Cybersecurity: financial crimes and fraud in the digital age

GOALS

Protect yourself and your organisation against cyber threats with this engaging and hands-on E-learning on financial crime in the digital age. This interactive e-learning is designed to increase your knowledge and put it into practice. In addition, you will develop your critical thinking skills, sense of responsibility and understanding of social engineering. The e-learning is designed as a documentary in which 2 hackers give you insight into their operation, techniques and tactics.

This training will enable you to:

- develop an in-depth understanding of social engineering and recognise the manipulative tactics used by cybercriminals;
- understand and identify various cyber attacks, such as phishing, deep fake and counterfeit software;
- apply your newly acquired knowledge in realistic scenarios using video material and interactive exercises;
- strengthen your skills to recognise weak passwords and use strong passwords;
- analyse and assess the trustworthiness of websites, emails and social media profiles;
- recognise and avoid the dangers of insecure Wi-Fi networks;
- detect suspicious activity;
- recognise social engineering tactics;
- report cyber attacks.

[Click here](#) to watch the trailer.

SUMMARY

Category:

- Compliance & audit

Difficulty level:

Advanced

Certification type:

E-learning

Price:

- Member: € 160.00
- Non member: € 180.00
- Partner BZB: € 160.00
- Incompany: custom tailored, prices on demand

CPD hours:

- Bank: **2h** general
- Insurances: **2h** general
- Consumer loans: **2h** general
- Mortgages: **2h** general
- Compliance: **2h**

INTENDED AUDIENCE

The training is suitable for professionals who want to increase their knowledge and protect themselves from the growing threat of cybercrime:

- employees who work online on a daily basis;
- managers responsible for the security of sensitive information;
- anyone who wants to improve their digital security.

FOREKNOWLEDGE

Advanced level training: this training requires a general basic knowledge of the subject.

CONTENT

CONTENT

- Introduction to cybercrime
- Social engineering
 - Learn what social engineering means and how it is used to manipulate people
 - Learn to recognise the psychological techniques and strategies behind social engineering
 - Strengthen your resilience against this form of cyber attacks and learn to apply effective defence mechanisms
- The weapons of cyber criminals
 - Explore the various tools and techniques cybercriminals use to gain access to systems and data
 - Learn about the risks of deep fake, counterfeit software and other advanced attack methods
 - Understand how cybercriminals exploit vulnerabilities of individuals & systems and what measures you can take to protect yourself
- Cybercriminals' attacks
 - Delve into the different types of cyber attacks, such as phishing, ransomware and macros
 - Learn how to recognise, prevent and mitigate these attacks
 - Develop a proactive attitude towards cybersecurity
- Security measures and incident response
 - Learn to apply essential security measures to protect yourself and your digital environment
 - Understand the basics of incident response and learn how to act quickly and effectively in the event of a cyber attack
 - Discover how to minimise your digital footprint and ensure privacy in a digital world

PRACTICAL INFORMATION

- **Duration:** 2 hours
- **Training material:** interactive module
- **CPD hours:** Each module includes an online test consisting of multiple-choice questions. CPD hours will only be granted if you pass the test. You are entitled to 2 attempts to pass the test. If you do not pass (result lower than 60%), CPD hours will not be granted for this (sub)module. We therefore recommend that you take the test only when you are sure you master the subject matter.

METHODOLOGY

An **'E-learning'** is 100% self-study. You log in individually on the MyFA learning platform and process, at your own pace, learning content that is provided to you via an interactive presentation. You can follow this online training wherever, whenever and as often as you want. The teaching material consists of a digital format with text, video, images, animations, test questions and/or references to relevant documents and/or websites.