Cyber training for accountants

Be able to confidently answer questions from your clients about information security. In this 4-hour course you gain a better understanding of cybersecurity.

About the accountants training

SMEs encounter cyber threats every day. This seems to hit SME companies particularly hard. No less than 36% of the SMEs in Europe were attacked at least once in 2021 via a phishing email and 13% had to deal with acquisition fraud.[1] Since the start of the pandemic, accounting firms have seen a 300% increase in cyber attacks.[2] Accountants, both in their own practice and with their clients, must be able to identify these cyber threats and respond appropriately.

This cybersecurity training is designed for accountants. The interactive classroom course covers the basic level of cybersecurity. Participants gain insight into the risks of digital crime and appropriate measures. This training provides a basis for answering frequently asked questions from customers and gives practical tools for your own practice. The aim is that your own practice and your customers are safer against digital crime.

Learning objectives

After completing the course, the accountant will be able to:

- Identify the importance of cyber security and develop a cyber security mindset
- Recognize cyber attacks (including data leaks, ransomware and fraud)
- Understand a cyber security framework, regulation and risk management
- Use a reporting framework for cybersecurity risk management in the audit process

[1] https://www.enisa.europa.eu/news/enisa-news/phishing-most-common-cyber-incidents-faced-by-smes
[2] https://www.naqcyber.com/blog/cyberattacks-on-the-rise-for-accountancy-firms

00 31 85 20 05 579
info@skopos.ai
www.skopos.ai

COURSE CONTENT

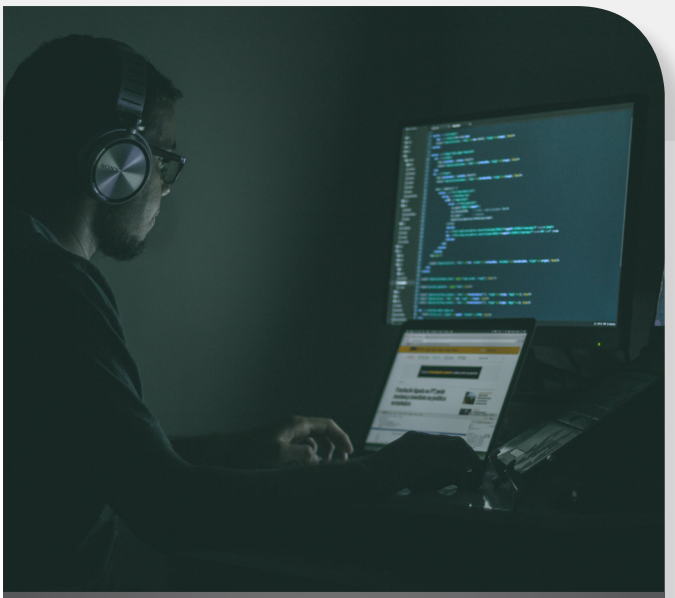
The accountant training consists of four modules.

Module 1:
Understanding the hacker: the importance of cyber security and developing a cyber security mindset

- Vulnerabilities in cybersecurity.
- Why do cybersecurity breaches take place and why are organizations susceptible to them?
- Current European cyber policy and global trends in cybersecurity activities.

Module 2:
The consequences of the cyber pandemic: data breaches, ransomware and fraud

- A cyber pandemic with major consequences.
- Case studies: A data breach, Ransomware, Fraud
- The basis of the following cybersecurity aspects: Protect, Detect, Respond.



TRAINING COST:
1750 € / 1490 £
(your office, all colleagues)
300 € / 260 £ (single registration)

TRAINING DURATION: 4 hours

Module 3:
A secure organization: framework and regulation

- The available cybersecurity frameworks
- Regulation and ethics in the field of data protection and privacy (including security standards such as ISO27001 and NEN7510).
- Information security assurance mechanisms.
- Policies for cybersecurity compliance and risk management

Module 4:
The consequences of the cyber pandemic: data breaches, ransomware and fraud

- A reporting framework for cybersecurity risk management.
- Policies, procedures and controls to mitigate the risk of loss from cyber-attacks.
- Practical application and simulation of audit process, cyber tips for accountants.
- Learn to ask and answer the right questions.
- Financial implications of cyber security.

Optional: Personalized training

For Skopos users, the training can be enriched with recognizable examples from the own organization by using the Skopos data.

Who is the course intended for?

- Management and accountants (partner/employee)
- Financial professionals
- CFOs and business managers

Sign up here

00 31 85 20 05 579
info@skopos.ai
www.skopos.ai