CYBERSECURITY AWARENESS IN MARITIME ENVIRONMENT

Delivery Method: eLearning || Duration: 1 hour || Course Fee: 100 €

Category: Cyber Security

Available language: English

Certificate

On completion of the training program, the student will be awarded:

- A Certificate of **Cybersecurity Awareness in Maritime Environment**, issued by Bureau Veritas Solutions Marine & Offshore.

The Certificate of **Cybersecurity Awareness in Maritime Environment** is obtained after completing the course and passing the online test.

Presentation

This training course provides general information about cybersecurity in the Maritime Industry. It describes the main cybersecurity issues regarding the use of computer-based equipment in the professional environment and proposes ways to protect oneself from hackers.

Whom the course is for

Crew cybersecurity training is an essential part of the cybersecurity risk management requested by IMO Resolution MSC.428(98), and to be implemented no later than the 1st of January 2021. The course **Cybersecurity Awareness in Maritime Environment** is aimed at anyone interested in understanding the general issues of cybersecurity in a maritime environment. It is mostly dedicated to crew but can be of great interest for: Shipowners, Masters, Officers of ships; Ships and Shipyards Technical Staff dealing with IT/OT equipment; Surveyors; etc.

Objectives

On completion of the training, students will be able to:

- Understand that we are living in a digital ultra-connected world;
- Know about main cyberattacks and ways to keep protected from them;
- Enforce main cybersecurity rules on ships;
- Understand Internet best practices and implement them;
- Be cautious when using social networks.

Program

- Digital revolution
  - Digitalization transforms the world, your environment, your work on ships
  - You are connected = you are vulnerable
  - Internet is NOT a lawless zone
- Cyberattacks on board and on a daily basis
  - What is ransomware, and how to react to it
  - How to use antivirus
  - How to care about and protect data
  - Why updates are necessary
  - Why be cautious with unknown Wi-Fi networks
- E-mail (professional and personal) best practices
  - How to recognize corrupted e-mails from legit ones
  - Think before you click
  - How to react to the detection of a suspicious e-mail
- Passwords
  - How to protect them, how to generate them
- Social networks
  - Have you become a “like” addict
  - Protect your e-reputation
  - Protect your Company e-reputation
- Your digital environment on board
  - Your ship is like a connected factory
  - How to react in case of a potential cybersecurity breach/incident