

Safe Internet Use on Boats (Basic Cyber Awareness)



Description: This 50-hour online program introduces participants to the fundamental principles of maritime cybersecurity. It focuses on safe Internet usage on vessels, the risks associated with public Wi-Fi in marinas, proper password

management, and the protection of crew devices. It is aimed at beginners, crew members, officers, technicians, and shipping company personnel.

Seminar Objectives:

- Safe Internet usage on ships and in marinas
- Recognition of basic cyber threats
- Creation and management of strong passwords
- Protection of personal and professional devices
- Avoiding risks from public Wi-Fi
- Identification of phishing and suspicious messages
- Implementation of security practices in daily work onboard

Target Audience:

- Crew members
- Officers and technicians
- Shipping company personnel
- New employees with no prior experience in cybersecurity

Course Modules (50 hours):

1. **Introduction to Maritime Cybersecurity (6 hours):** What is cybersecurity, basic threats on ships, real-life incidents, why beginners are targets.

2. **Safe Internet Usage on Ships (8 hours):** Internet via satellite, risks from insecure networks, separation of crew and operations, what to avoid.
3. **Public Wi-Fi in Marinas and Ports (8 hours):** How hotspots work, Man-in-the-middle attacks, password theft on open networks, secure connection practices, use of VPN.
4. **Strong Passwords and Access Management (6 hours):** What makes a password strong, password managers, Two-Factor Authentication, avoiding common mistakes.
5. **Protection of Crew Devices (8 hours):** Security of mobile phones and tablets, software updates, antivirus and firewalls, safe USB usage, risks from social media onboard.
6. **Phishing, Scams, and Suspicious Messages (6 hours):** Recognizing phishing emails, examples of attacks, what to do with a suspicious message, safe use of links and attachments.
7. **Simple Security Practices (8 hours):** Rules for safe browsing, safe use of the cloud, personal data protection, actions during a cyberattack, daily security checklist.

Learning Outcomes:

- Safe Internet usage
- Strong passwords
- Protection of devices and data
- Identification of suspicious activities
- Reduction of the risk of cyberattacks onboard