SecAwareness Truss

#3 Newsletter

# Kickstarting 2026
# Elevating Cybersecurity Training for Critical Infrastructures

**Happy New Year to our community!**

**2026** marks the year SecAwarenessTruss moves **from design to real-world validation**. This edition highlights our comprehensive training framework, the cornerstone of our mission to fortify Europe's critical sectors - Energy, Telecoms, Health, and Maritime - against evolving cyber threats.

## Our Strategy: Core, Cross-Domain and Sector-Specific Training

Our training approach is built on **three distinct pillars** to ensure comprehensive coverage.

We provide **Core modules** for foundational security, **Sector-Specific scenarios** tailored to the unique needs of our four pilots, and **Cross-Domain Delivered Programmes** designed for horizontal exchange.

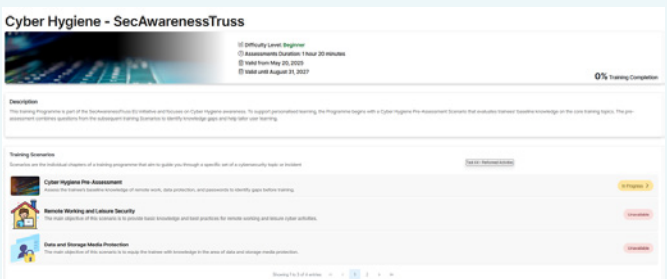
This structure enables a strategic exchange of expertise, ensuring that security insights from one field can directly enhance the resilience of another.

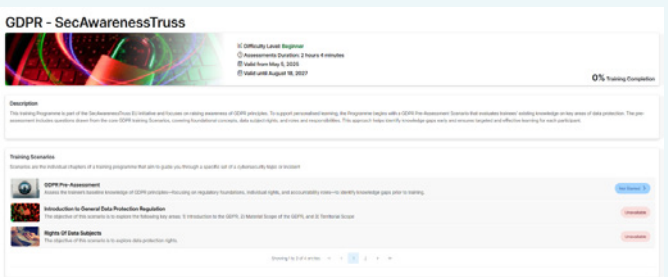
## Our Training Programmes at a Glance

### 1. Core Training Programmes

Horizontal modules to build a strong foundational security culture.

- **Cyber Hygiene Programme:** Practical, scenario-based training covering essential security practices for everyday digital environments.
- **GDPR Compliance:** Hands-on scenarios guiding participants through data protection principles, rights and organisational obligations.
- **Fostering Organisational Awareness:** Awareness training for office personnel and IT teams, focusing on physical and information security risks.
- **Understanding OSINT & Social Engineering:** A specialised programme demonstrating how publicly available information can be exploited and how to defend against social engineering attacks.



## 2. Cross-Delivered Training

Pilot-driven programmes delivered across all sectors to promote strategic knowledge exchange.

- **DDoS Attack:** Detection, Response & Recovery: A high-pressure simulation addressing volumetric, protocol, and application-layer attacks on critical services.
- **NIS2 Regulation Compliance:** Practical guidance on implementing the NIS2 Directive, covering risk management, governance, and incident reporting.
- **Recognising and Preventing Phishing Attacks:** Interactive scenarios enhancing employees' ability to detect and respond to phishing via email, SMS, and voice.

## 3. Sector-Specific Training

Advanced, technical scenarios tailored to the unique operational environments and technical challenges of our four pilot domains.

### Healthcare Sector

- **Privilege Escalation and Lateral Movement**
- **Cross-Site Scripting (XSS) Attacks in Web Applications**

### Energy Sector

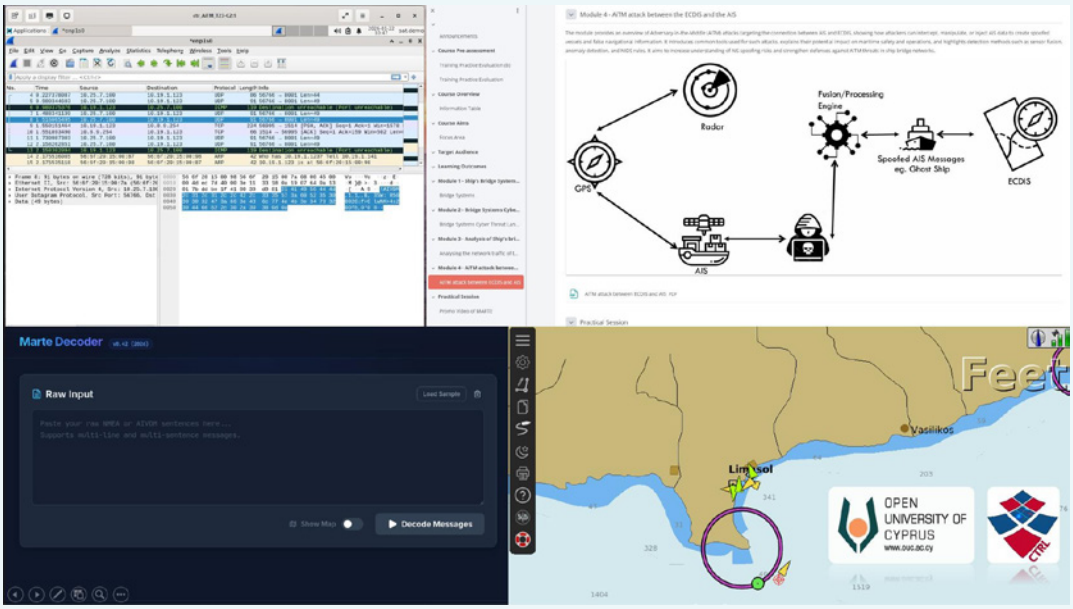
- **Mitigating Man-in-the-Middle Attacks on AMI**
- **Rogue AMI Headend DoS Attack Mitigation**
- **GPS Spoofing on Wide Area Measurement Systems**
- **Physical Security Awareness in Energy Facilities**
- **Data Privacy and Confidentiality for Energy Personnel**

### Telecommunications Sector

- **Persistence Attacks and Golden Ticket Exploits in Active Directory**
- **Protecting Sensitive Data in Daily Operations**

### Maritime Sector

- **Ransomware Defense for Maritime Navigation**
- **OSINT Vulnerabilities in Port Systems**
- **Maritime Cybersecurity Regulations**
- **Enhancing Awareness of the Maritime Cyber-threat Landscape**
- **Addressing Data Manipulation on Fleet Management Systems**
- **Detecting and Responding to AIS Spoofing**




## What's Next in 2026

The coming months will see the full-scale deployment and evaluation of these programmes through our **Cyber Range infrastructure.** Stay tuned as we begin the hands-on validation phase with our partners in Greece and Cyprus, marking a key milestone in the project's lifecycle.

Interested in a specific training module? **Get in touch with us to learn more!**

Subscribe to our newsletter to receive exclusive updates and expert content delivered straight to your inbox.

# A Dynamic Training Experience for Critical Infrastructures based on Cyber-Ranges

For the latest updates and insights, be sure to follow us on social media.

**Connect with us**

SecAwarenessTruss Project

**Visit our website**

https://secawarenesstruss.eu/

**Stay connected, stay informed!**

**Co-funded by the European Union**

This project has received funding from the European Union's Digital Europe research and innovation programme under Grant Agreement No 101128049.

**Be part of our growing community!**