Sec Awareness Truss

#6 Newsletter

From Training Delivery to Lasting Impact

Strengthening Cybersecurity Preparedness Across Critical Infrastructure Sectors

A Major Milestone in Cybersecurity Training

As SecAwarenessTruss approaches its final implementation phase, the project has reached an important milestone: all 22 training programmes have been recorded as delivered across its four critical infrastructure pilot sectors: Healthcare, Energy, Telecommunications and Maritime.

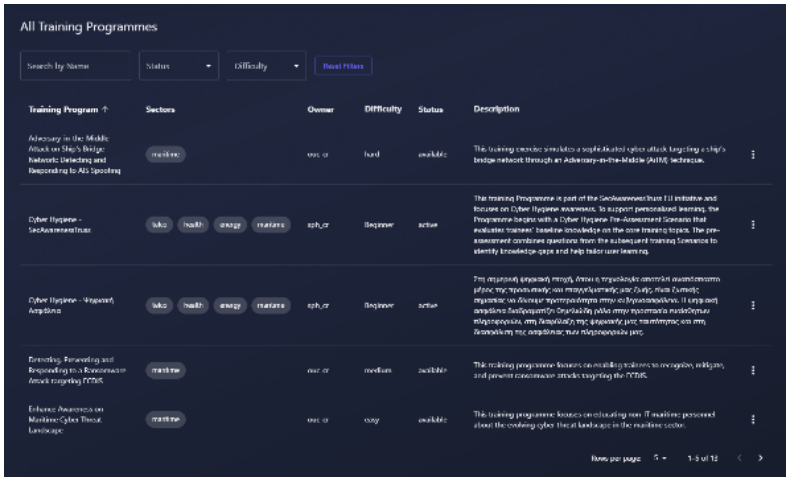
Combining foundational cybersecurity awareness, specialised technical knowledge and realistic cyber range scenarios, the training portfolio addresses sector-specific threats while promoting a common understanding of cybersecurity risks and responsibilities.

This edition highlights the achievements across the four pilots and looks ahead to the evaluation and consolidation of the project's results.

Training Delivery at a Glance

The SecAwarenessTruss training portfolio comprises three complementary categories:

- 4 Core Training Programmes, covering essential cybersecurity awareness and organisational security practices.
- 15 Sector-Specific Training Programmes, tailored to the operational challenges of Healthcare (2), Energy (5), Telecommunications (2) and Maritime (6).
- 3 Shared Training Programmes, addressing common cybersecurity challenges, including DDoS attack simulation, NIS2 compliance and phishing awareness.



Cybersecurity Training Across Four Critical Sectors

Through tailored training programmes and realistic cyber range scenarios, SecAwarenessTruss has addressed cybersecurity challenges across four critical infrastructure sectors.

Healthcare Pilot

The Healthcare pilot, represented by PAGNI University Hospital, has delivered specialised training addressing Cross-Site Scripting (XSS) attacks and Privilege Escalation and Lateral Movement in healthcare information systems. Complemented by shared training on DDoS attacks, phishing awareness and NIS2 compliance, these activities support the protection of sensitive information and essential healthcare services.

Energy Pilot

The Energy pilot, represented by PPC Group, has delivered training covering DDoS attacks, Man-in-the-Middle attacks targeting Advanced Metering Infrastructure (AMI) and GPS spoofing affecting Wide Area Monitoring Systems (WAMS). Additional programmes on physical security and data privacy address the protection of both operational systems and sensitive information.

Telecommunications Pilot

The Telecommunications pilot, represented by OTE Group, has focused on Persistence Attacks and Golden Ticket Exploits in Active Directory, alongside the protection of sensitive data in daily operations. Shared training on DDoS attacks, phishing awareness and NIS2 compliance complements these activities, addressing both technical threats and everyday security practices.

Maritime Pilot

The Maritime pilot, jointly supported by the Digital Security Authority (DSA) and the Open University of Cyprus (OUC/CTRL), has delivered six specialised programmes addressing ransomware threats, AIS spoofing, data manipulation in fleet management systems and OSINT-related vulnerabilities in port environments. Additional training on maritime cyber threats and cybersecurity regulations further strengthens sector-specific awareness and preparedness.

Building Cybersecurity Awareness Across Sectors

In addition to specialised technical training, SecAwarenessTruss has delivered core and shared programmes addressing common cybersecurity challenges across critical infrastructure organisations.

Covering topics such as Cyber Hygiene, GDPR, Phishing Awareness, NIS2 Compliance, Physical and Information Security, and OSINT-related Social Engineering Risks, these programmes reinforce the importance of secure everyday practices and employee awareness.

This combination of technical and awareness-based learning reflects the project's commitment to addressing cybersecurity from both an operational and human perspective.

Looking Ahead

Following the delivery of its training portfolio, SecAwarenessTruss is focusing on evaluating training outcomes, collecting participant feedback and consolidating the results achieved across the four pilots.

The remaining activities will focus on finalising project deliverables, identifying lessons learned and exploring opportunities to ensure the continued value and use of the project's training resources beyond its completion.

Upcoming Plenary Meeting in Cyprus

The SecAwarenessTruss consortium is scheduled to gather in Nicosia, Cyprus, on 19-20 November 2026, for its next physical Plenary Meeting, hosted by the Digital Security Authority (DSA) at the ICT Academy. The meeting will provide an opportunity for project partners to review progress, coordinate the remaining activities and discuss priorities as SecAwarenessTruss approaches its final milestones.

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!