

Title: CyberMyths Bridging Cybersecurity with Cultural Legends

Timeline: 24 Months

Field: Cooperation Partnership in Youth

Budget: € 250.000

The Content : In the modern era, where digital interactions permeate every aspect of our lives, understanding cybersecurity has become paramount. As technology continues to evolve at a breakneck pace, the threats associated with it have also grown in complexity and sophistication. Cybersecurity learning, therefore, is not just a specialized field for experts but a necessary discipline for every digital citizen. While traditional cybersecurity education programs provide a strong theoretical foundation, graduates often find themselves ill-prepared to tackle the complexities of the rapidly changing cybersecurity landscape. Theoretical knowledge alone is insufficient in the face of real-world challenges, which demand practical application and adaptive problem-solving skills.

Highlighting the significance of cybersecurity knowledge and its far-reaching implications, enhancing digital skills and competence development for particularly young entrepreneurs, individuals, startups, businesses and societies at large. Digital Culture project not only focuses on increasing cyber security competences, taking actions in any situation when encountered cyber threat or attack and preparing for future profession but also creates synergies between cultural heritage and cyber security resilience among young entrepreneurs supporting the active citizenship of the participants and their cultural and historical heritage.

The Objectives of The Project:

1. Train young people who can prevent, detect and analyze cyber security incidents and have knowledge and skills at the level of expertise about process management.
2. Explore the vital role of hands-on activities in cybersecurity and its impact on young people
3. Highlight the dual importance of cybersecurity and cultural heritage in today's digital world.
4. Enhance cybersecurity proficiency and general awareness of cultural heritage among young people.

Target Groups: Higher Education students studying at digital technologies

Young Entrepreneurs and Startups, SMEs

Youth Workers

The Challenges and Needs Faced in Cyber Security Field

1. A global shortage of skilled cybersecurity professionals,
2. In theoretical cyber security trainings learners understand what knowledge is needed to execute tasks and responsibilities but lack of experience about how to execute and implement in reality, thereby helping young cyber security students and youth workers master complex cybersecurity concepts and equipping them with the practical skills are urgent need to succeed in their future careers.

Activities:

1. Project Management
2. Development of Cybersecurity Scenarios
3. Scenario-Based Assessment and Question Preparations
4. Organization of the Cybersecurity Competition
5. Post-Competition Analysis, Evaluation, and Dissemination of Results