It is known that many companies, employers, and employees are not prepared for numerous cyber-attacks, so an increased focus on defensive measures has a high priority on global policy, national security agendas, and education.

National Initiative for Cybersecurity Education (NICE) (https://www.cisa.gov/nice-cybersecurity-workforce-framework) underlines that in many important areas “an integrated cybersecurity workforce” is necessary also due to many complex cyber-attacks. There is a severe need for cybersecurity talent, suitable education, and training facilities to develop new ones to solve such complex problems as cybersecurity ones.

Cybersecurity is interdisciplinary - professional research shows that security activities contain vital elements of social, legal, ethical, sociological, psychological, and technical, but also economic and managerial ones. Not all security professionals as well as managers and employees understand all of these fields that influence careers, so it is expected that organized teaching and training facilities will contribute to developing interdisciplinarity.

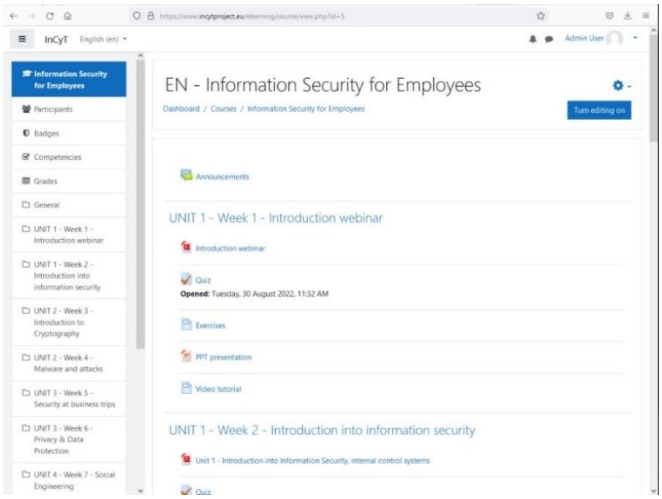
In this context, within the Erasmus+ project Interdisciplinary Cyber Training (InCyT) the partners from University, research, VET, and SMEs, developed a digitally interdisciplinary training program supported by a collaborative digital platform for small and medium-sized companies (SMEs). SMEs in particular are objectives for criminal activities also due to less knowledge about cybersecurity measures and connections with other disciplines. SMEs' resources are limited, so they need help.

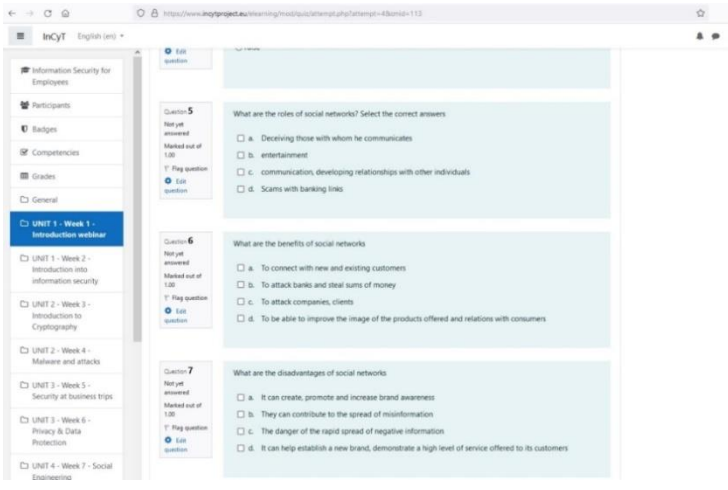
This training program will be adapted for VET and a European transferability model is planned. According to interviews and short studies done at the beginning of the project, the program is structured across two modules, one for Managers, and one for Employees, where each module consists of a number of units and topics. Besides text, the modules contain streaming Webinars, Quizzes, and self-assessment exercises and those answers will be put on discussion forums.

The developed training modules are the following:

1. Introduction into Information Security, internal control systems
2. Cryptography Fundamentals
3. Malware
4. Security at business trips
5. Privacy & Data Protection
6. Social Engineering / SPAM / Phishing
7. Security and Privacy in Social Networks
8. Information security management
9. Third party / vendor security
10. Cyber risk and resilience

The following pictures shows some examples how the digital platform supports the training.





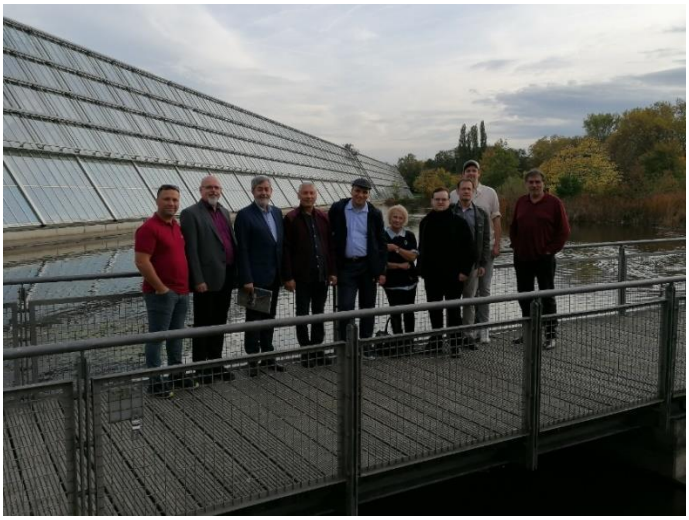
Co-funded by the Erasmus+ Programme of the European Union

Call 2021 Round 1 KA2
KA220-VET - Cooperation partnerships in vocational education and training
Form ID KA220-VET-E0B193D2

At the end of the training, the learners should develop an electronic portfolio to organize their work and present their learning experiences. These serve as training assessment tools, provide opportunities for learners to start thinking about what they learn, and give employers the possibility to "know" what students learned.

Students should respond to questions like: What did you like the most about the training?, What helps at most to learn the material?, Please describe anything you didn't like about the training, Were materials and the digital platform easy to be used in the training? , Can you use the learned skills and knowledge in your job?

At the face-to-face meeting in Gelsenkirchen, Germany (27-28 October 2022, see pictures below), the partners discussed improvements in training modules. Another topic of the meeting was to make known the training program within SMEs from partner countries and the strategy to find learners who would like to follow the training: employers and employees.



The training program will start at the beginning of December 2022 and takes 4 months: two weeks for every training module. The learners will be supported by a mentor in each partner country. The mentor will organize a session once a week during the training time, promote work in a group and support the learners in doing exercises.

The project partners continue the dissemination activities i.e. some presentations at conferences:

INTERDISCIPLINARY CYBER TRAINING

THE FUTURE OF EDUCATION, POWERED BY 5G-BASED IT AND AI

09.11.2022, Antalya, online

IEEE 20th International Conference on Information Technology Based Higher Education and Training

ITHET 2022, Ileana Hamburg

SELECTED CYBERSECURITY ISSUES - CHALLENGES AND RISKS

05.10.2022, Astana, on-line

A Development Day - seminar on the problems related to cybersecurity, Dominik Strzalka

The next meeting will be held in Copenhagen: