Erasmus+

Digital Competences for Improving Security and Defence Education (DIGICODE)

KA226 Strategic Partnerships for Higher Education: 2020-1-PL01-KA226-096192

CYBERSECURITY REQUIREMENTS FOR E-LEARNING PLATFORMS IN DIGITAL SECURITY AND DEFENCE EDUCATION – IMPLEMENTATION OF ONLINE COURSE

– INTELLECTUAL OUTPUT 03

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

Schumen, 2022

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

PRESENTERS

Name, surname	Institution
Linko NIKOLOV	"Vasil Levski" National Military University, Artillery, Air Defence and CIS Faculty of Shumen, Bulgaria
Radostin DIMOV	"Vasil Levski" National Military University, Artillery, Air Defence and CIS Faculty of Shumen, Bulgaria

Disclaimer: The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the National Agency and Commission cannot be held responsible for any use which may be made of the information contained therein. The authors of this document have not performed illegal activities – all analysis is made over controlled test environments, having all partner institutions agreement. The GDPR regulation must be kept during reading this document.

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

CONTENT

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

1. CYBER ATTACK VECTORS

The DIGICODE project had developed a “Teacher’s tool-kit” using internet-based e-learning system for educational purposes as an Intellectual Output 02. E-learning platforms trend to increase their impact across educational institutions. On one hand, it appears as an improovement and evolution of educational process. On the other hand, as an online service, the cybersecurity risk is imposed. Lots of vulnerabilities may be found while performing online education.

The cyber attack vectors include preliminary techniques used by hackers with the aim to gain access to assets – information, systems etc.

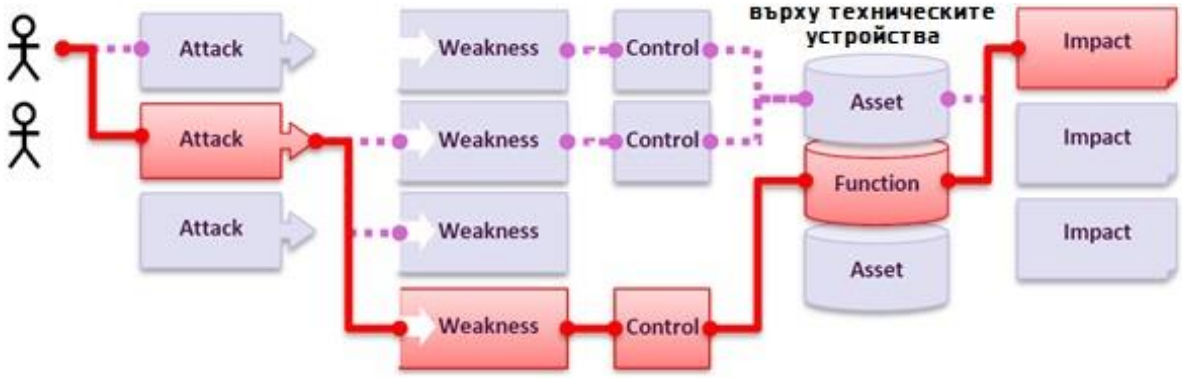
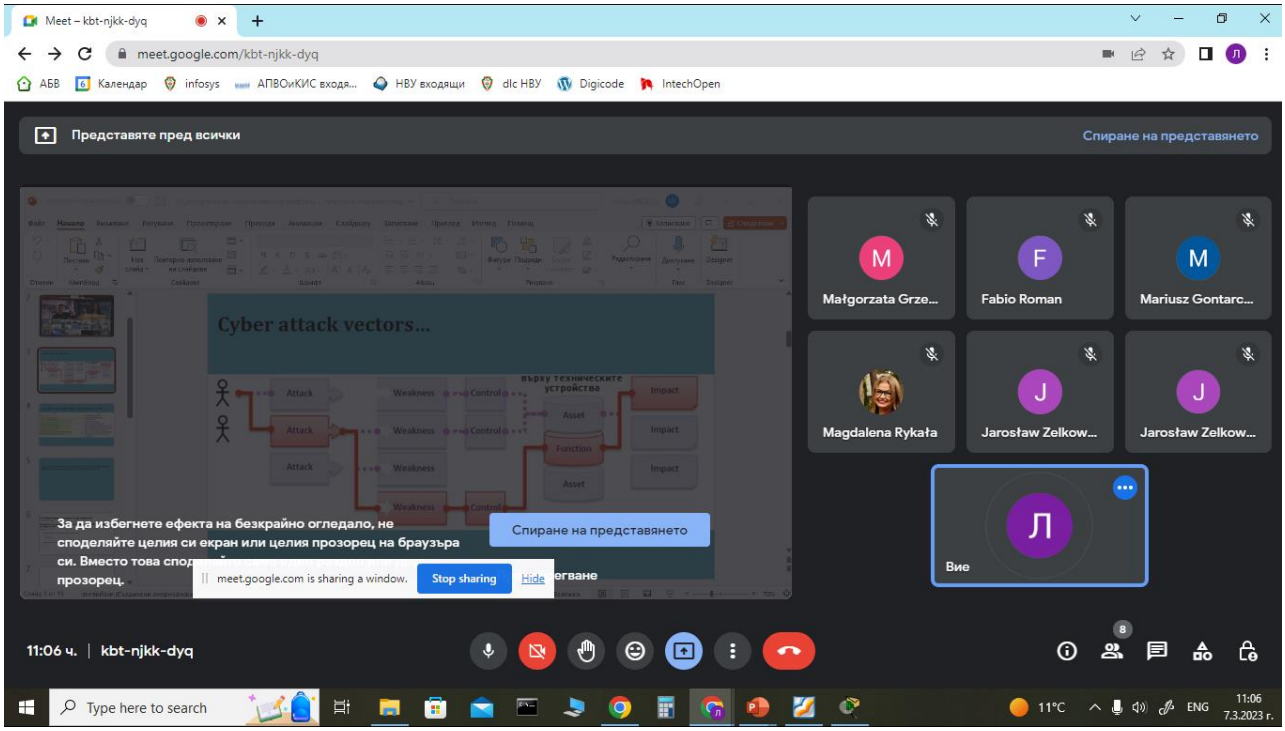


Fig. 1 – The cyber kill chain [OWASP, https://owasp.org/]



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

Common and popular attacker access attempts

- Login pages with fake passwords. Scammers create sites that look like login pages (for e- learning account, e-platform, cloud services, etc.) and then include links to them in phishing messages.
- **Fake password login pages.** Fraudsters create sites that look like login pages (for e-learnin systems) and then include links to them in phishing messages.

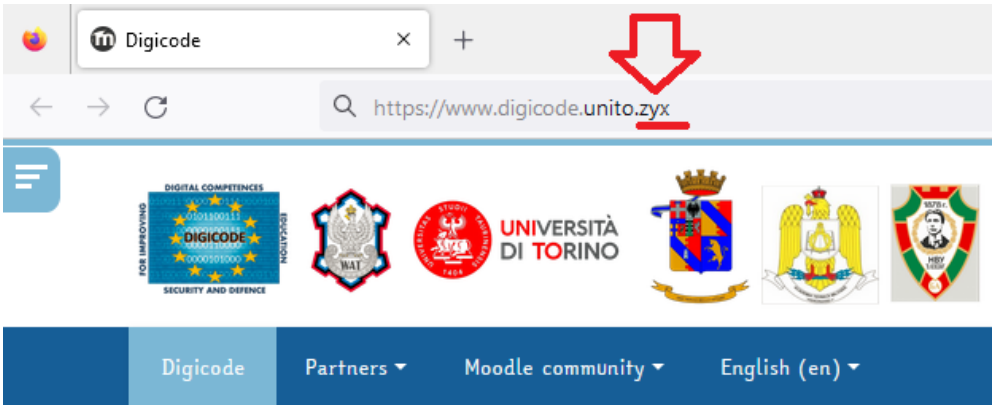


Fig 2 – Fraudulent domain

- **Malicious pop-ups that download malware.** Hackers create pop-ups on legitimate websites that download malware onto student's device. Once installed, they can spy on them or scan their hard drive for sensitive information.
- Fake customer support websites. Scammers pretend to be from technical support companies and get s student to give them remote access to their computer.

Fig. 3 - Notifications of PC security vulnerabilities

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

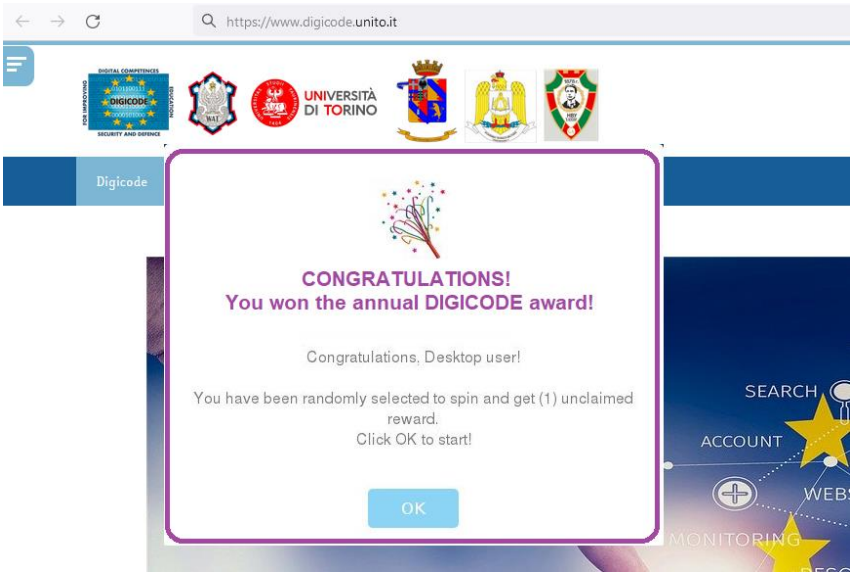


Fig. 4 – Malicious announcements about profit, bonus, reward, etc.

If such messages are received, the students should scan their system for potential threats or contact an administrator before taking any action.

Brief advises for Social Engineering Attacks prevention:

Humans are prone to make wrong decisions because of their emotions. That's why educational organizations need a social engineering plan to fight against attacks, safeguard their data, and keep their students out of danger [16].

Education – Make sure that e-learning system has a well-documented security policy, and these policies should be taught every studnet so that they are aware of social engineering attacks before using the account.

Penetration Testing – It is a common practice for some e-learning platforms to issue a task for the network security engineer to penetrate one network by following some of the standard practices of social engineering. For example, sending an email from a spoof email to all the students will reveal the ground of the implementation of security policies.

Multi Factor Authentication – Enhancing how e-learning security layers for studnets to access systems and data can help in avoiding social engineering attacks. Combining passwords with biometrics, for example, is one way that multifactor authentication can beat the criminals at

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

their own game.

Updating Antivirus and Anti-Malware Software – It is strongly recommended for the students' computers to regularly update their antivirus and anti-malware. Solid antivirus and anti-malware protection will prevent malicious links and downloads from reaching students' mailboxes in the first place [16].

In such an insecure online environment, penetration tests are fundamental method for assessing the cybersecurity of communication and information systems. As the hackers are trying to gain unauthorized access to the systems, these tests perform the same methods, attacks and procedures to estimate the cyberhealth of the targeted e-learning environments. The evolution in cyber defence system offers Artificial Intelligence (AI) with Machine Learning and Deep Learning [7] but those systems undergo further development.

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

2. ATTACK SCENARIO IN PREDEFINED TOPOLOGY.

If a hacker is eavesdropping the network communication session, he may find vulnerable processes and can create a specific payload (virus, malware) for a given scenario. The DIGICODE poposed tool-kit platform offers internet access to a dedicated server and online learning platform. Havin internet connection is the reason it should be considered vulnerable.

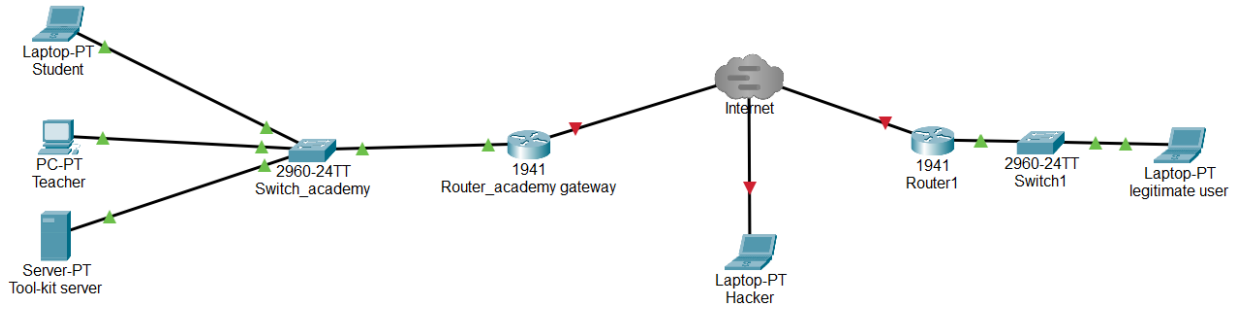
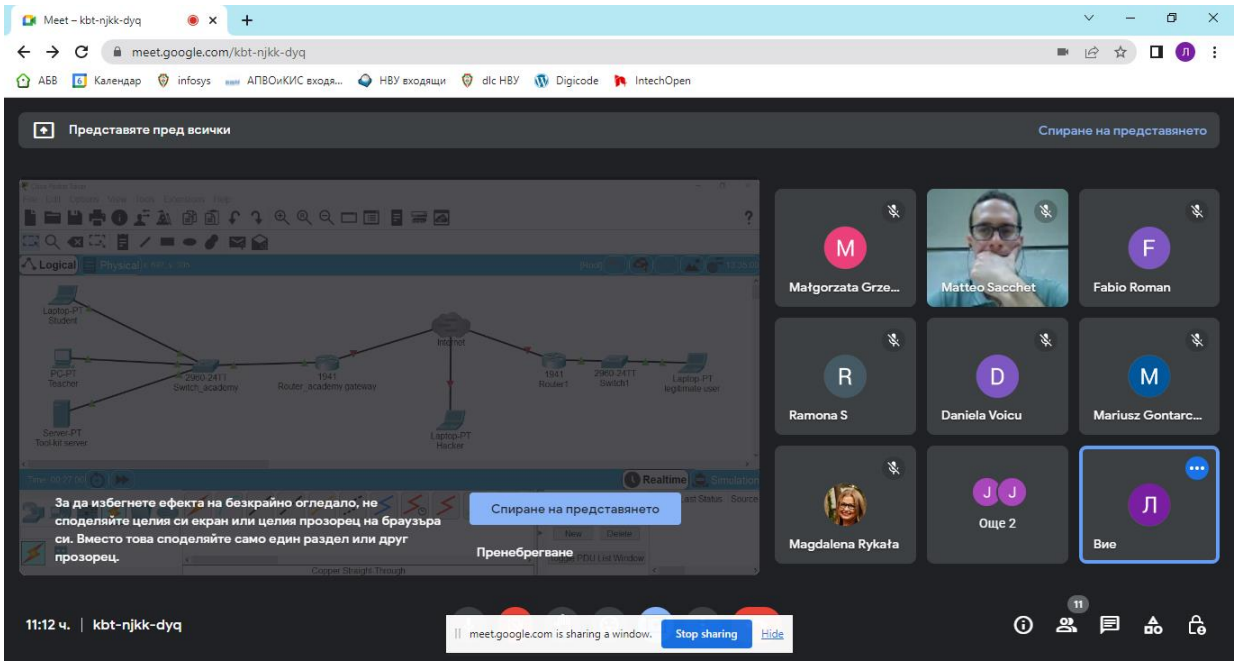


Fig. 5 – An example of network topology



Common Social Engineering Attack Techniques:

Attackers use various techniques to play with the human mind of the student or trainee, using their unexperienced internet behavior. The most common methods are:

Phishing Attacks - This technique focuses on sending emails to a large number of people to reveal personal details such as their password. The emails look like they are from a legitimate

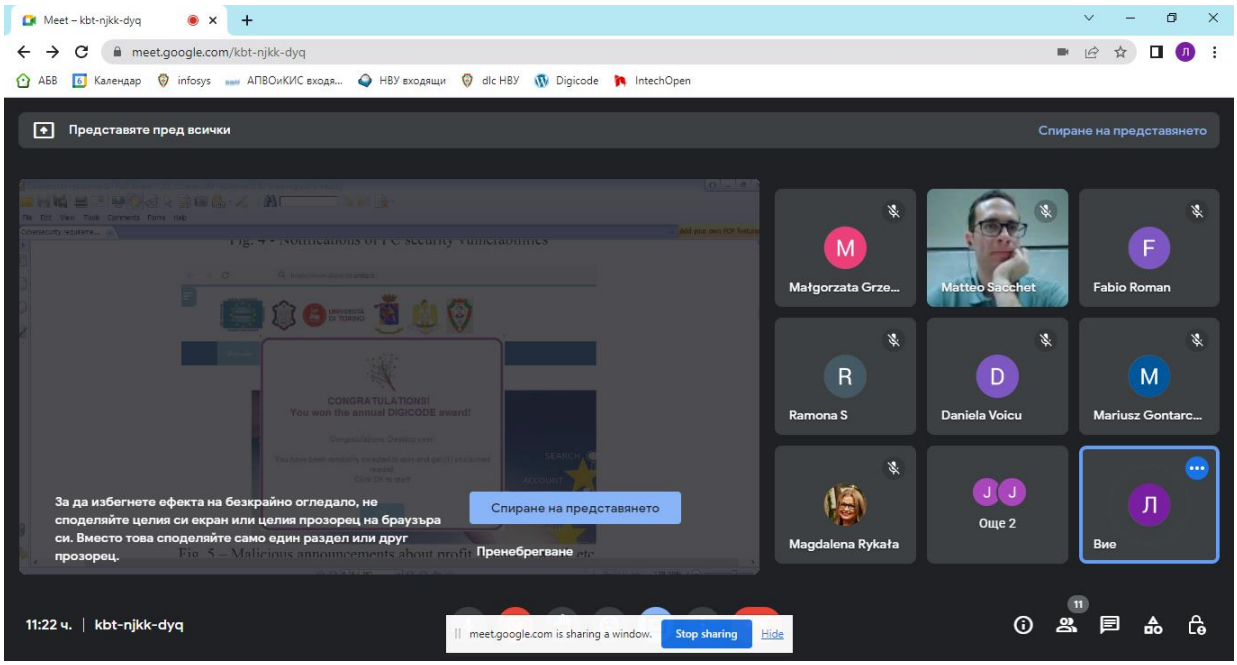
Co-funded by the Erasmus+ Programme of the European Union

source of the e-learning, and some students can easily fall into this trap if they do not read the email carefully.

Spear Phishing - Spear phishing is similar to phishing, but the target audience is narrowed down to a specific group of people or an individual like a student. For example, the attacker may ask the trainee to send a payment to his offshore bank account.

Psychological Manipulation - While executing a social engineering attack, attackers exploit human emotions such as helpfulness, greed, fear, and obedience. If a student is not able to control his feelings, the attackers will gain access to the information they need (in minutes) and will never be caught.

Trust Factor - Many students trust their friends or family members with their personal details. This is precisely why some attackers target them through the email accounts of the people they believe. They'll send them malicious links through such email accounts, and when a student downloads them, their job is done.



.

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

3. CYBERSECURITY POLICY AND REQUIREMENTS FOR E-LEARNING PLATFORMS.

The goal of cybersecurity policy and requirements definition is to acheive cybersecure infrastructure and safe online experience. The most higlhy required activities as an e-learning user are to perform the following:

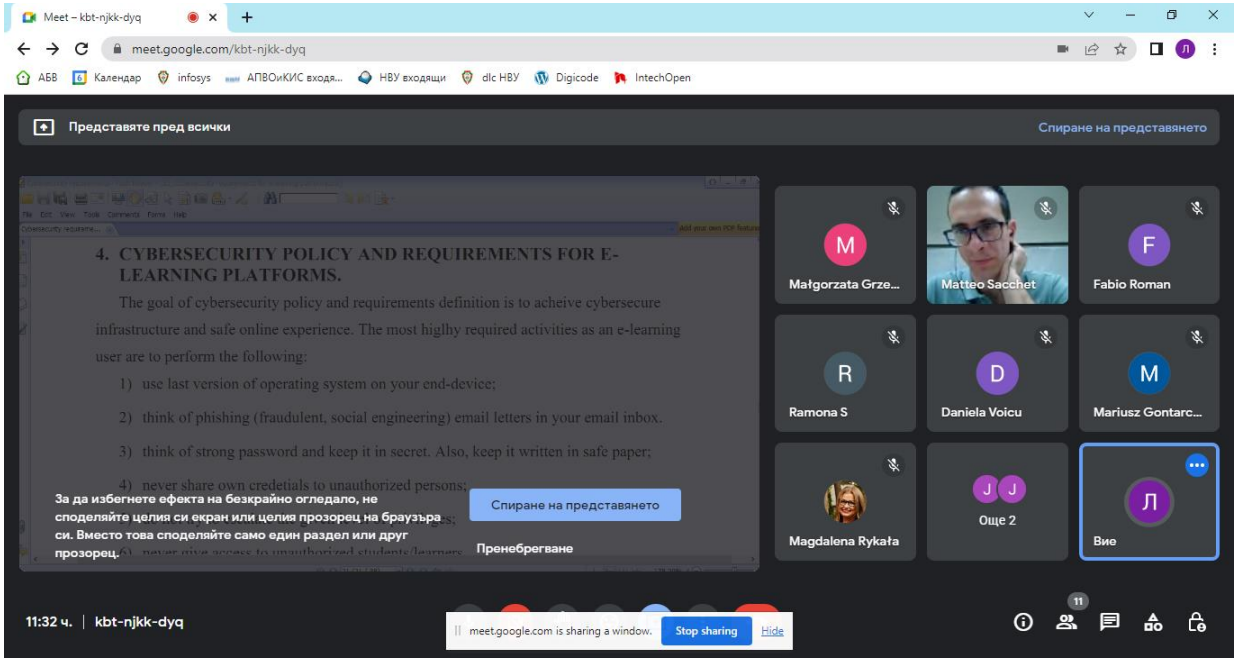
1) use last version of operating system on your end-device;
2) think of phishing (fraudulent, social engineering) email letters in your email inbox.
3) think of strong password and keep it in secret. Also, keep it written in safe paper;
4) never share own credetials to unauthorized persons;
5) do not try to escalate the given level of privileges;
6) never give access to unauthorized students/learners.

Anti-Malware Policy:

All e-learning end users are required to use a licensed version of an antivirus programme that must cover the following essential aspects:

- Be capable and reliable of detecting and destroying both already known and unknown (zero-day) malware.
- To provide real-time protection - scanning of running programs, identification and blocking of programs with detected malicious behavior.
- To provide malware protection for the organization's e-learning environment.
- To achieve the goals described above, students should use a programmatic antivirus solution to detect, destroy and protect against malware. The product must be installed on all workstations to work with the e-platform.
- The following minimum requirements for the programmatic antivirus solution used by the organization are in effect:
- The software antivirus solution must function in real time on all workstations on which it is installed. The product is configured to provide real-time protection.
- The database of antivirus definitions of the software antivirus solution used is configured to perform an automatic update at least once a day.
- The software antivirus solution is configured to perform a periodic automatic scan, at least once a day.

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



Activities for anti-virus protection required from all e-learning end users:

- maintain the most current version of the currently used anti-virus solution on all workstations that are used to access the system.
- ensuring the installation and running of the current version of the software anti-virus solution, as well as its stable operation.
- take care of the presence of the software anti-virus solution on the computer systems falling within the scope of its activity.
- In case of infection with malware that is not destroyed by the software antivirus solution, the platform administrator and server administrator must be notified immediately, including the measures taken to identify it and disconnect the infected machine from the infrastructure.

Special requirements for all users when handling passwords:

- The password is personal and is not shared with anyone else.
- Students are required to create strong passwords that are difficult to crack and that do not contain dictionary words or information about users (such as user IDs, names of family members, dates of birth, etc.)
- If the password is suspected to be compromised, it is changed immediately,
- It is forbidden to store the password on paper and in easily accessible places, the relevant employee is responsible.

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

- The user is obliged to protect the disclosure of his password when entering it into the system,
- The user can change his password at any time, but only once a day;
- Ability to change the password when it has expired,
- Students should not reuse already used passwords according to the information in User Password Requirements.
- Passwords given by the System Administrators/Help Desk must be changed by the user immediately after the user logs into the system. New users are provided with an initial one-time password and existing users are provided with a new password according to the password policy.
- The provision of passwords is controlled through the established administration process detailed in Access Administration Process. Help Desk must validate users' identity before performing a password reset.
- In case of absence for a long period of time exceeding 30 days (maternity leave, business trip abroad, long-term treatment, etc.), the student's user ID is blocked and activated upon his return. Information about such trainees enters the e-learning organization.
- Shared or group user IDs are not allowed (must be disabled).

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

4. FINAL REMARKS

By this online course the aim was to introduce to all participants the needed awareness for cyber threat actors and the possibilities of being hacked. Despite the technical systems used to bring cybersecurity at decent level, proper education is still the best weapon against cyber attacks.

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