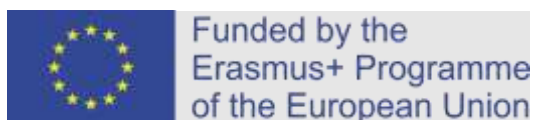# Safeguarding Against Phishing in the 4th Industrial Revolution (CyberPhish)

# A2: Guidelines for Implementation

**Project Duration**: November 2020 – November 2022

**Project No.:** 2020-1-LT01-KA203-078070

# Contents

# 1. INTRODUCTION

In the age of the 4th Industrial Revolution, cyber security is becoming one of the biggest challenges. The widespread use of digital devices and information systems is increasingly attractive to cyber criminals. According to Eurostat data, "...in 2019, approximately one in three EU citizens aged 16 to 74 reported security-related incidents when using the internet for private purposes in 2019 in the last 12 months. During this period phishing was the most frequent security incident reported in 2019". In practice, no information system or security software can provide 100% protection against phishing attacks. The fight against these threats is not only about hardware and software security solutions, but also about the user's resilience to such threats and their ability to recognise them.

Cyber-attacks are also targeting businesses in Europe. According to the 2017 Global State of Information Security Survey, around 80% of European companies experienced at least one cyber security incident that year, and employees were responsible for 27% of all cyber security incidents.

So only a human – a user who understands how a cybercriminal operates and can recognise the warning signs of malicious activity, can help prevent cyber-attacks such as phishing.

According to ENISA, cyber-related subjects are underrepresented among non-technical programmes students. It is, therefore, relevant to develop and offer to the public a widely accessible online training course on how to identify phishing.

For these reasons, the international project "Safeguarding against Phishing in the age of 4th Industrial Revolution" (CyberPhish) was initiated and implemented. The European Union funded the project under the Erasmus+ programme. The project was coordinated by the Kaunas Faculty of Vilnius University, with Tartu Ulikool (Estonia), Dorea (Cyprus), MECB (Malta), Altacom (Latvia) and the Institute of Information Technology (Lithuania) as project partners. The project duration is from November 2020 to November 2022.

The main aim of the project "CyberPhish" is to educate higher education students, lecturers, university staff (community members), education centres, and the business sector (employers and employees), and to promote critical thinking in the field of cyber security among the target group.

The Cyberphish project aims to develop a curriculum, e-learning materials, a blended learning environment, simulations, self-evaluation and knowledge evaluation tests. Developed CyberPhish course enables users to protect against phishing attacks. Users acquire competencies that will help them to pay attention to threats and to take the necessary prevention measures.

The project has developed an intellectual product for training users' critical thinking and skills in identifying phishing. Users will learn to recognise phishing signs (red flags), social engineering techniques and cyber security skills. The blended learning approach/concept will allow users to prepare for a knowledge test and receive a certificate of completion.

The project partners used the online learning platform covering training material, simulations, self-evaluation tests and knowledge evaluation tests in the pilot training in five partner countries. On the basis of this experience, these guidelines have been developed.

**Purpose of the Guidelines**

The present guidelines are intended to present the project results, the best piloting practices and a methodology for developing a CyberPhish training course for the target audience and stakeholders. The guidelines are addressed to organisations interested in adapting and using the developed material to educate Internet users in phishing recognition: higher education institutions, adult education/training centres, business sector.

**Objectives of the Guidelines**

The main objective of the Guidelines for implementing of "CyberPhish" is to present the tools, content and process of organising the training. During this process, participants acquire the knowledge and skills needed to identify phishing attacks at work and in their personal lives and prepare for a knowledge test. They will be awarded a certificate upon successful completion. The implementation process is based on the experience of the participating partner countries.

# 2. CYBERSECURITY, FISHING AND SOCIAL ENGINEERING

## 2.1 Cybersecurity and Fishing in study programmes

Since 2013, the European Commission has been highlighting the importance of the issue of cybersecurity. The first Cybersecurity Strategy highlights awareness-raising and skills development as key strategic objectives. The 2017 ENISA Report also highlights the importance of cybersecurity. It recommends that EU Member States strengthen cybersecurity education and skills (ENISA, 2019, p. 23). As a result, all EU Member States have developed and published their National Cyber Security Strategies (NCSS).

In March 2021, the European Council adopted new conclusions on the EU Cybersecurity Strategy[1]. The findings recognise the shortage of digital and cybersecurity skills and underline the need to meet market demand by further developing education and training programmes.

The CyberPhish project surveyed existing curricula and training programmes in cyber security and phishing in the partner countries Cyprus, Estonia, Latvia, Lithuania and Malta. DOREA Educational Institute led the study. The main findings of the study were:

- The analysis of HEI study programmes in all project partner countries except Estonia does not include phishing and social engineering topics as separate modules. However, one can incorporate information about these topics in other course modules. Two HEI study programmes in Estonia include study modules focused on social engineering. The average duration of such modules is 4,5 ECTS.
- The analysed HEI study programmes in Estonia, Latvia and Malta include course modules in soft skills, such as communication skills, entrepreneurship, psychology, etc. Contrary, HEI study programmes in Cyprus and Lithuania are mainly focused on hard skills, putting less emphasis on the importance of soft skills.
- In all partner countries, a few public and private organisations offer training courses in cybersecurity targeting Cybersecurity and IT professionals, companies, employees, and the general public. While the shorter duration training courses tend to focus solely on threats, including phishing, social engineering, and ways to protect oneself, longer duration training courses provide a broader perspective on cybersecurity. There are also some organisations offering penetration and social engineering test targeting companies and their employees.

The data gathered from the survey helped to identify skills gaps and to develop recommendations for a new training programme, CyberPhish. This programme aims to enhance the skills and awareness of internet users and educate them on the latest cyber security issues and threats, particularly phishing.

## 2.2. Recognising Phishing and social engineering

Cybersecurity is also an issue for European businesses. Companies are increasingly becoming targets of cyber-attacks. As criminals become more sophisticated, cyber-attacks are becoming more challenging to detect and prevent, and new methods and platforms are being used to carry out such attacks. According to the 2017 Global State of Information Security Survey, around 80% of European businesses experienced at least one cyber security incident that year. According to the survey, employees are responsible for 27% of all cybersecurity incidents. In Q1 2019 alone, companies worldwide were targeted by cyber-attacks 120% more often than in 2018 and suffered massive losses (€22.2 billion).

As Human Factor Report 2019 states, more than 99% of emails distributing malware require human intervention, i.e. following links, opening documents, accepting security warnings, and other behaviours [5].

It is therefore essential to educate and raise awareness in this area. Cyber resilience requires explaining/teaching how to identify phishing in a way that is understandable and accessible to most people. Knowing the warning signs and understanding the methods of criminals will firstly make internet users feel more confident and secure, and secondly, help them to prevent, or at least slow down, the spread of such attacks.

---

[1] Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy (accessed 09/09/2022)

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

Phishing is illegal to extort a user's personal data (login credentials, credit card information, etc.) using social engineering techniques. Criminals are active on social networks, sending emails and making phone calls. These messages aim to persuade the user to open a malicious attachment or click on a fake web link, revealing their password. [6]

The most common types of phishing are Spray and pray, Cat phishing, Advanced fee scam, Spear fishing, Whaling, Vishing, Smishing, Angler Phishing, Clone Phishing, and Malvertising.

In the context of information security, social engineering is defined as the psychological manipulation of people into performing actions or divulging confidential information. ENISA states that social engineering remains a top threat to facilitate other types of cybercrime, as 84% of cyber-attacks rely on social engineering. The number of phishing victims continues to grow since it exploits the human dimension being the weakest link [6]

Social engineering techniques rely on human weaknesses such as greed, fear, curiosity, trust, empathy, and haste. Therefore, a carefully crafted and personalised email, voicemail, phone call or text message can influence people to reveal their confidential information, click on a malicious link, download and open a file containing malware, or even transfer money to the criminal.

Dr. Robert B. Cialdini in his book "Influence: The Psychology of Persuasion", described six principles of persuasion which were readily adopted and used in social engineering and phishing. Later they were expanded to seven: Reciprocation, Scarcity, Authority, Consistency, Consensus, Liking, and Unity. Fraudsters using such techniques can expect successful results from the attacks they create. It is, therefore, particularly vital to educate people so that they know how to recognise and avoid such attacks. [7; 8; 9]

Project partners carried out a survey to find out how people recognise phishing attacks, to identify people's awareness of phishing and different types of phishing, and to identify the skills gaps in the partner countries Cyprus, Estonia, Latvia, Lithuania and Malta. The results of the study are available in the Study Report "Recognising Phishing and Skills Gaps". [7]

Five hundred fourteen people took part in the survey, of which 259 were women, 248 men, and 7 people preferred not to identify their gender. Most respondents are students (304), followed by employees (139), business owners (53), unemployed people (10) and self-employed people (8). Most survey respondents are highly educated – with the majority of respondents (38%) having a bachelor's degree, followed by a master's degree (23%) and a PhD (6%).

Interestingly, almost one in five respondents reported having been the victim of a phishing attack in the past. The most common phishing attacks have occurred when clicking on links in emails or messages, opening attachments or replying to emails and providing confidential data. The most common reasons for these attacks were distraction, curiosity or haste. Most respondents (74%) have not attended any cyber security training or seminars. More than half of the respondents (54%) indicated that they had developed an interest in this field independently. All this shows a growing need for knowledge on phishing and cybersecurity.

## 3. CYBERPHISH CURRICULUM

Based on a needs analysis, the consortium of partners has developed a training curriculum on cyber security, cyber-attacks, social engineering, with a particular focus on identifying and preventing phishing.

The aim of the Curriculum is to provide an introduction to cyber security, with a focus on phishing attacks. The course programme is aimed at individuals, students, entrepreneurs, employees of organisations, and will prepare them for the security threats of the fourth Industrial revolution age. The course will provide learners with the skills to identify and manage cyber-attacks and to protect devices and data.

The curriculum is designed for blended learning, but its structure makes it flexible and can be used for both distance and face-to-face training. The full training programme consists of 30 hours corresponding to 1 ECTS. It is being suggested that the same number of hours per module are to be considered for self-study and assessment.

The curriculum is structured in four distinct parts (modules):

1. Introduction to Cybersecurity;
2. Overview of Cybersecurity within the EU;
3. Cyber-attacks – Social Engineering and Phishing;
4. Understanding and Handling Cyberattacks.

The full Curriculum can be found on CyberPhish website: https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2_Extended-version-of-curricula_EN.pdf

# 4. CYBERPHISH PILOT TRAINING ORGANISING

The pilot training is designed to train participants to identify phishing attacks, understand social engineering, and learn new and improve existing skills. The application specifies that the products developed during the project must be piloted to evaluate the results and, if necessary, to adjust them in the light of comments and feedback from participants and teachers/mentors.

**Participants**. The pilot training took place in all project partner countries – Cyprus, Estonia, Latvia, Lithuania, and Malta. Participants included:

- Higher education students,
- Staff from higher education institutions and organisations,
- Teachers and staff from adult education centres.

Each partner organisation trained at least 24 participants in its country, thus extending the impact of the project beyond its own organisation.

**Duration**. By agreement between the partners, the pilot training lasted several months (May-September), taking into account the summer holidays of each partner. Some partners were able to hold the pilot training at the end of the academic year, i.e. in May, at the end of the spring semester. Other partners could start at the beginning of the academic year in September and gather the participants for the pilot training by the end of September.

**The way**. The pilot training can be organised as a blended learning course or, given the constraints of the Covid-19 pandemic, can be organised remotely.

Vilnius University and University of Tartu piloted the training in their own organisations, integrating the Cyberphish course into their study subjects. The other partners, Altacom, Dorea and MECB, conducted the pilot training in cooperation with other higher education institutions or by inviting external participants.

**Learning platform**. The learning platform CyberPhish was developed and tested in five languages - English, Estonian, Greek, Latvian, Lithuanian and Lithuanian. Participants had to familiarise themselves with the developed learning material, take self-evaluation tests after each topic of the course, solve simulations, and take a final knowledge test.

**The organisation of pilot training**

Before the pilot training, the five partners agreed to organise the training in their countries to ensure that:

- at least 24 participants from each partner country complete the pilot training (at least 120 participants in total across all countries);

- the participants complete a pre-pilot questionnaire, i.e. to assess their existing knowledge before the training (at least 120 completed questionnaires in total);

- the final knowledge test is considered to be passed when the participant scores at least 75%;

- participants will complete a questionnaire at the end of the pilot training, i.e. to assess their existing knowledge after the training (at least 120 completed questionnaires in total);

- at least one trainer from each partner country will also complete the questionnaire on the training (at least 5 questionnaires). This questionnaire will help to evaluate the project's pilot training. The answers (feedback) given by the trainers will provide information on the quality of the course developed, i.e. the relevance of the topics to the target audience, the comprehensiveness of the course topics, the structure and the content of the course material, and the length of the training. The most important question will be to what extent the course has achieved its objective of introducing the audience to cyber security and fraud.

- At the end of the pilot training, each partner will submit a summary of the pilot training to the Coordinator. The Coordinator will use this information to prepare the IO6 report. Partners will make updates to the intellectual outcomes (IO2, IO3, IO4 and IO5) following the synthesis of the results of the pilot training.

## 5. RESULTS OF THE PILOT TRAINING

The pilot training occurred in five partner countries –Cyprus, Estonia, Latvia, Lithuania and Malta. A total of 229 participants took part in the training. One hundred seventy-five (175) participants completed the training with a 75% or higher score.

## Pre-pilot questionnaire

Before the pilot training started, all participants completed a pre-training questionnaire to assess their initial knowledge of fraud and cyber security. A total of 229 participants completed such pre-questionnaires. The breakdown of participants by country is shown in the figure below.
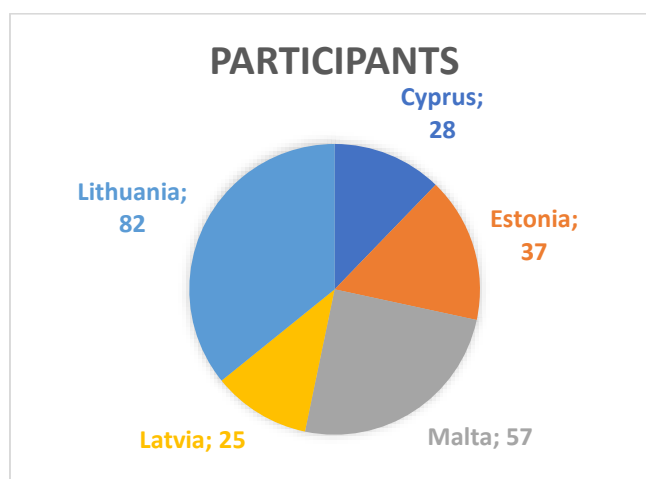


*Figure 1. Pilot training participants by country*

**An initial level of participants' knowledge before the training**

The questionnaires were analysed to assess the participants' pre-training knowledge in the pilot training. The figure 2 shows the distribution of the participants according to the scores obtained. 27% of the participants' knowledge were poor about phishing (score is less than 5 points). The same part (27%) of the participants had only a basic knowledge (i.e. the score 5-6 points). 25% of the participants had a score of "moderate" (7 points). 15% of the participants had knowledge evaluated as "good" (i.e. 8 points), when only 6% of the participants had a score of "very good" (9 points or more). Participants' knowledge was assessed on a ten-point scale.
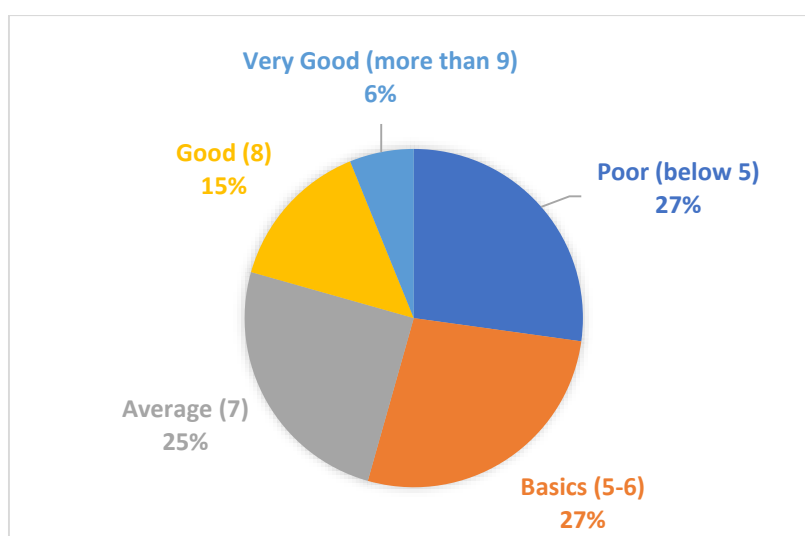


*Figure 2. Knowledge of the participants in the pilot training before the training*

The figure 3 shows the distribution of participants' knowledge (as scored) before the pilot training on a ten-point scale. Figure 3 shows the distribution of participants' knowledge (on a 10-point scale) before the pilot training.  It can be seen that just over a fifth of the respondents scored highly (i.e. scores of 8, 9 and 10).
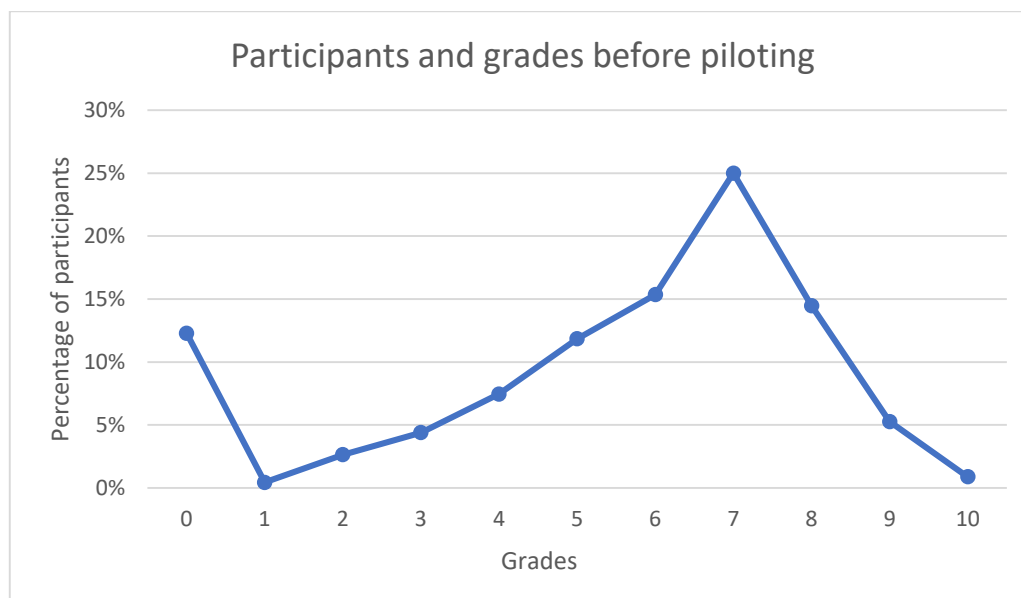


*Figure 3. Distribution of knowledge score by participants in the pilot training*

**The difficulty of questions: 5 most straightforward questions**

Analysing the participants' questionnaires showed which questions were tough and which were easy enough. Based on the answers provided by the participants, we have identified the five most straightforward questions. Approximately 70-75% of all participants answered these questions correctly. These questions are shown in the table below.

| |
|---|
| **Top 1. 15. Is it true that phishing attack is performed are only by email?** |
| **No**<br>Yes |
| **Top 2. 13. Which actions can prevent from social engineering attacks?** |
| **All listed**<br>Know what your personal information is available online<br>Use multifactor authentication<br>Enable spam filter<br>Keep software up to date |
| **Top 3. 5. Which one covers best the scope of the term "cyber-attack"?** |
| **Any malicious activities in cyberspace, even if they are unsuccessful**<br>Harmful actions via internet<br>Sending viruses and trojans via email or SMS messages<br>Successful phishing attacks |
| **Top 4. 12. Social engineering is** |

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

**Manipulation of people, usually through psychological persuasion, to gain access to information systems or data.**

attack which uses a malicious program that is hidden inside a seemingly legitimate one

malware that threatens to publish the victim's personal data or perpetually block access to it unless a fee is paid

when an attacker intercepts a two-party transactions, inserting themselves in the middle

a type of program installed to collect information about users, their systems or browsing habits, sending the data to a remote user

**Top 5. 14. What are the tactics used in phishing emails?**

**Request to send confidential information by email**
**Please click on the link in the email**
Providing information about the number and results of successfully performed phishing attacks during last year
Asking to donate for cleaning the ocean
Request to contact the sender by phone

*Table 1. The easiest questions for participants (Top 5)*

The first question is about fraud tools. The second is about prevention measures. The third is about the definition of cyber-attacks. The fourth is about social engineering, and the fifth is about fraud tactics used in emails.

So, we can see what the participants had enough knowledge of before the training.

**Pilot training: the complexity of questions: the 5 most challenging questions**

The analysis of the answers provided by the participants identified the most difficult questions to answer. These questions were not answered or responded poorly by 60-80% of participants. These questions are shown in the table below.

**Top 1. 7. What is the purpose of a Cyber Security Certification Framework?**

**Certify ICT products, processes and services**
To provide certification for obtained cyber security competences recognisable across EU
To provide ICT certification recognisable outside EU
None of provided answers

**Top 2. 8. Which directive was the first piece of EU-wide cybersecurity legislation to introduce security requirements as legal obligations for Digital service providers (DSPs) and operators of essential services (OESs)?**

The e-Privacy Directive
The EU Cybersecurity Act
**The NIS Directive**
European Electronic Communications Code Directive

**Top 3. 3. Which statements about phone phreaks are correct?**

**Phone Phreaks learned to control the phone lines by listening to the sounds as calls were connected by operators**
**Phone Phreaks read phone company technical journals**
Phone Phreaks were not breaking into offices to develop their own hardware
Phone Phreaks don't dig through telephone company trash bins to find "secret" documents

**Top 4. 4. What is the difference between cybersecurity and computer security?**

**Cyber security captures different fields of IT**
they are the same
cybersecurity is part of the computer security
cybersecurity deals only with Internet threats
cybersecurity is about viruses, etc.

| Top 5. 11. Which statements about Phishing Attack are correct? |
|---|
| **Phishing is a social engineering scam that can result in data loss, reputational damage, identity theft, the loss of money, and many other damages to peoples and organisations** |
| **A phishing scam usually starts with an email trying to gain the potential victim's trust and convince them to take the attacker's desired actions** |
| Phishing is a characteristic of a system asset that can constitute a weakness or a flaw in terms of system security |
| Phishing describes a standard means by which a threat agent carries out a threat |

*Table 2. The most difficult questions for participants (Top 5)*

The first question was about the purpose of a cybersecurity certification scheme; the second question was about the benefits of encryption; the third question was about the characteristics of a compromised device; the fourth question was about the NIS Directive; the fifth question asked about the differences between cyber and computer security.

As can be seen, the questions dealt either with technical topics or with specific issues such as the cyber security framework or the Directive.

# Online learning environment

The pilot training is conducted in a system developed and maintained by the project coordinator Vilnius University. The system can be accessed via the link https://cyberphish.vuknf.lt/. The learning platform can be used by both registered and non-registered participants. Non-registered participants can view general information about the training course, view rating tables and view or download training materials in all partner languages: English, Estonian, Greek, Latvian and Lithuanian.



*Figure 4. Online learning environment*

*Figure 5. Learning material in the online learning environment*

**The three roles of an online learning environment**

There are three user roles in an online learning environment: administrator, local administrator and course participant.
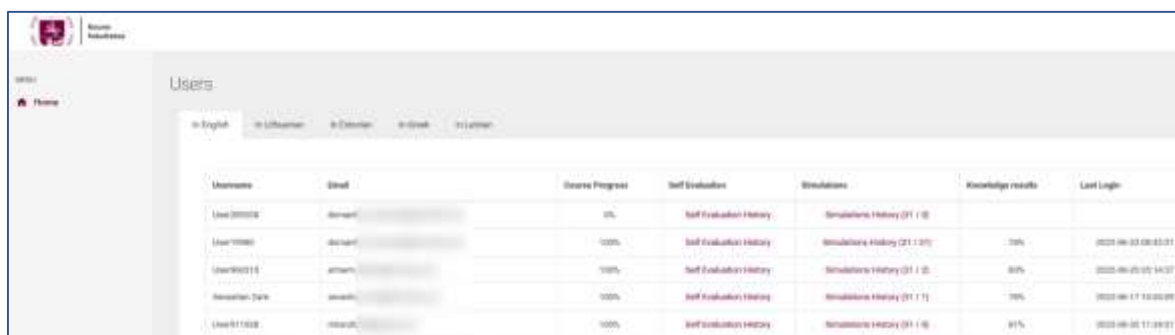
**The administrator** can view statistical information of all users, such as last login, IP address, status, and email address.
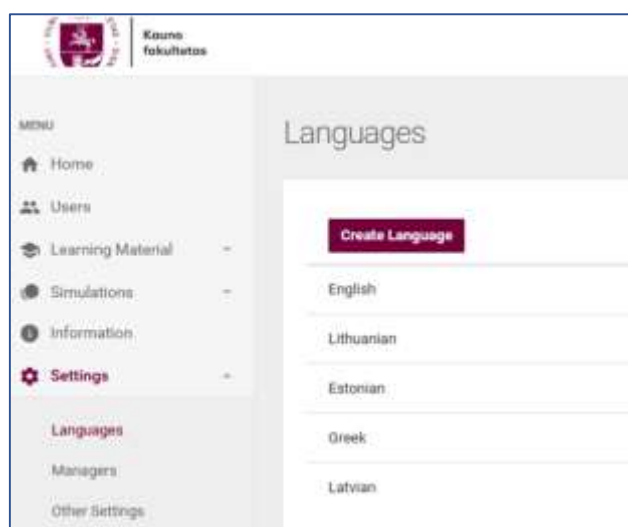


*Figure 6. System administrator window*

**The administrator** can upload training material, import and edit simulations, create local administrator users and specify other actions related to the e-platform that are unavailable to other users.

**The local administrator** can see statistical information about users' progress, as well as information about self-assessment tests taken, and simulations solved, last login and knowledge assessment test results. The user can also view solved self-assessment questions and scenarios, see how the participant solved a particular scenario and how many points they scored for each answer.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
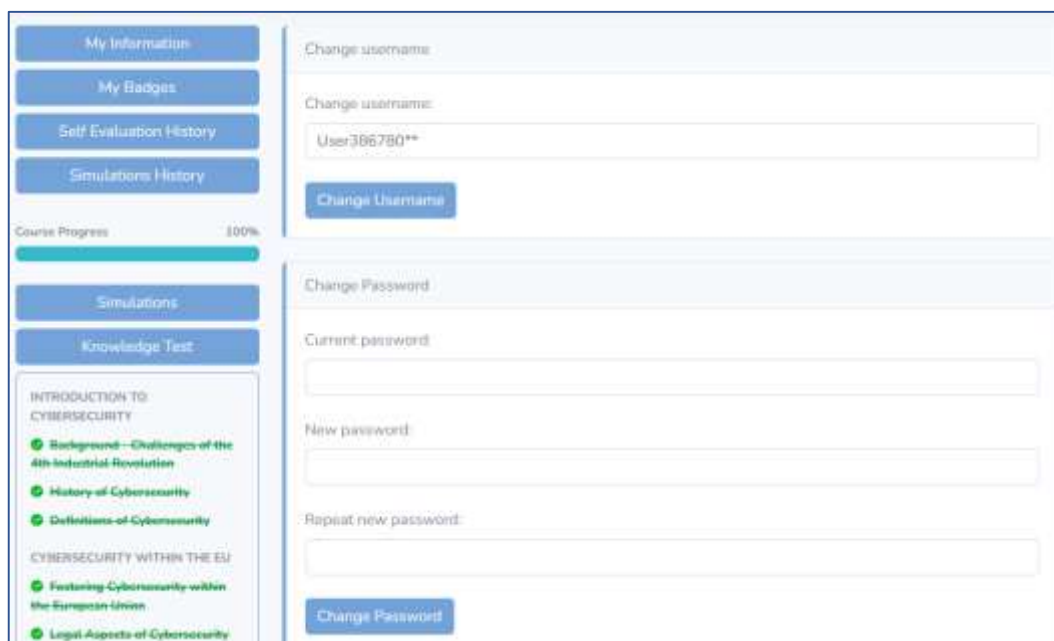Safeguarding your digital future



*Figure 7. Local administrator window*

**The registered course participant** can use the learning environment for learning purposes. Figure 8 shows an example of a course participant window.
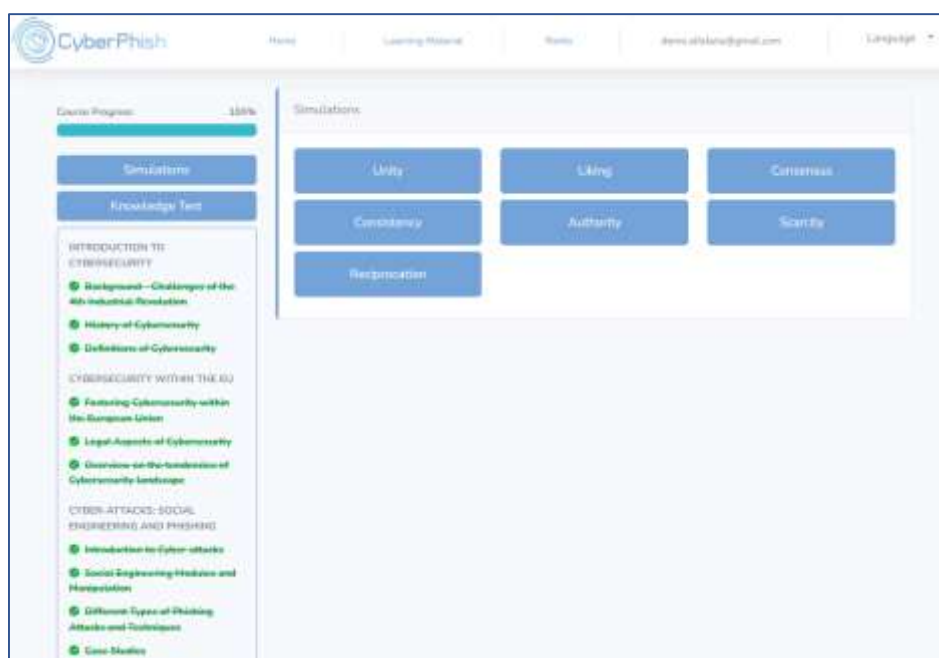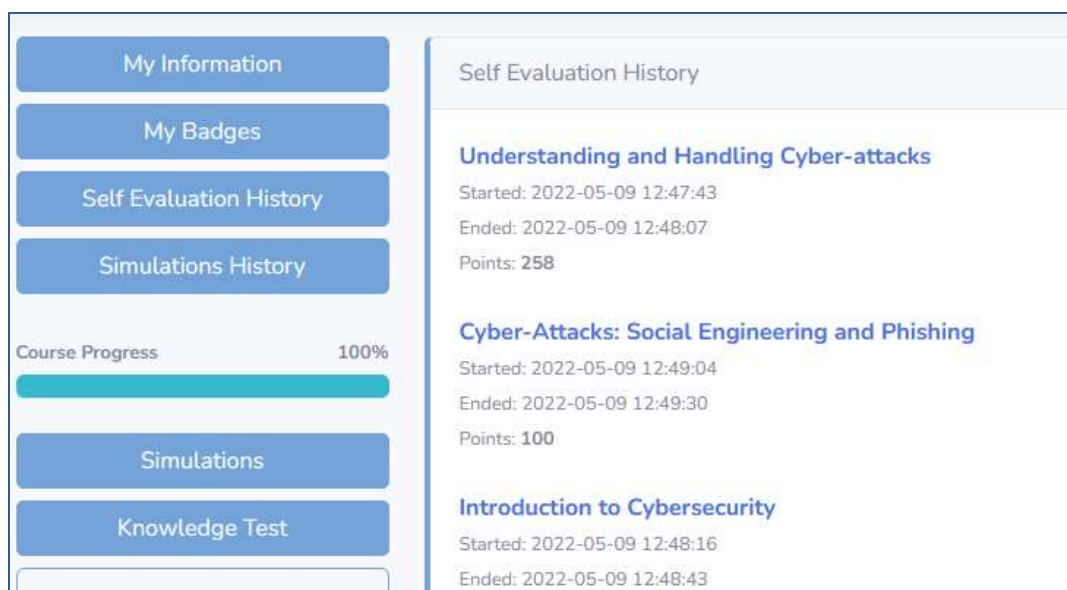


*Figure 8. Course participant learning environment window*

Once registered for the course, participant can change the information about yourself, i.e. username and password (see Figure 9).

*Figure 9. Window for setting the course participant's personal information*

As a registered course participant, you can keep track of your self-test history, and knowledge test history and see how many badges you have earned (see Figure 10).



*Figure 10. Course participant self-evaluation test history window*

As a registered course participant, you can keep track of the history of the simulations you have completed/solved:

- when and how you answered the questions;
- Which scenarios you solved;
- How many points you scored for each of them.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

*Figure 11. Course participant simulation history window*

**Badges**

Before the pilot training, the partners agreed on six badges. Still, during the project eight badges were created:

- passing the test;
- completing the course;
- completing all the simulations;
- giving the first self-assessment test;
- completing the category and the topic;
- achieving all the presentations;
- logging into the system every day for ten days.

Figure 12 examples of badges.



*Figure 12. Examples of Badges*

**Scoring**

Registered course participants can collect points for self-tests according to rules agreed by the partners. These scores are displayed in the Self Evaluation Ranks table. The course participant's name and the collected are displayed together.



*Figure 13. Rankings of registered course participants*

**Learning material in an online learning environment**

Partners consortium developed the online training material following CyberPhish Curriculum[2] and according to the 4th Industrial Revolution needs. Developed learning material was well evaluated by independent experts (one per partner country).

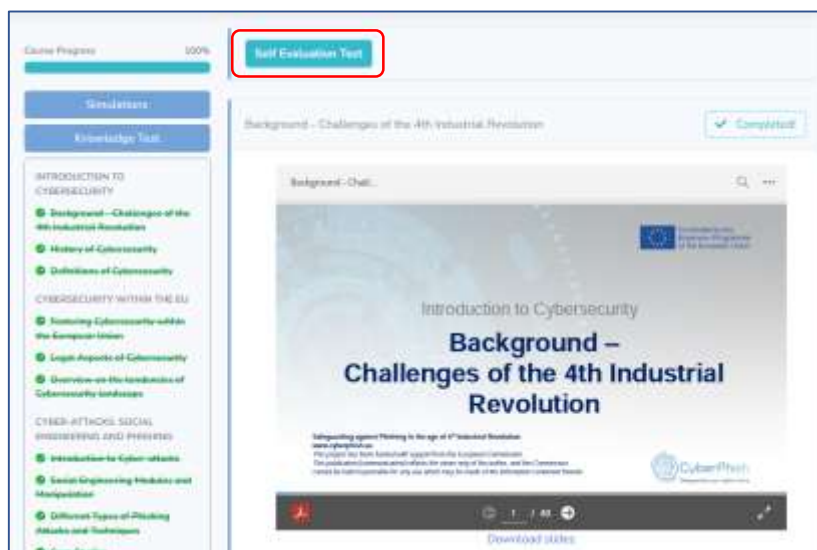The table 4 below provides a summary of the training material developed.

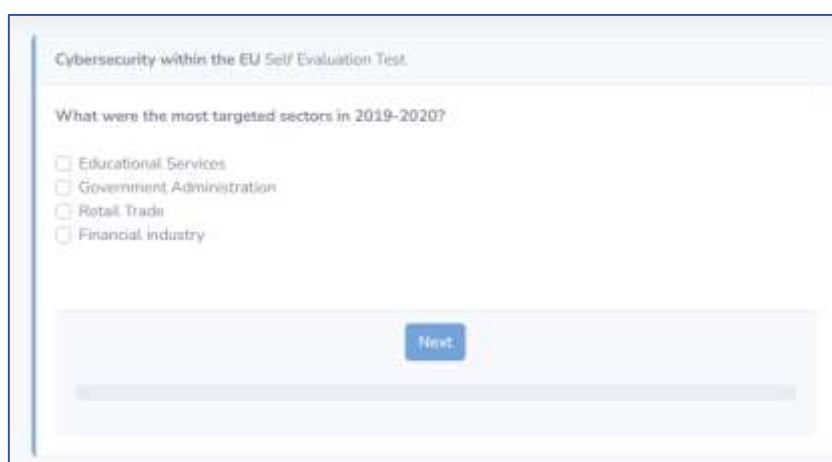| | Modules and sub topics | | | Number of slides |
|---|---|---|---|---|
| 1 | **An Introduction to Cybersecurity** | 1.1 | Background – Challenges of the 4th Industrial Revolution | 40 |
| | | 1.2 | History of Cybersecurity | 31 |
| | | 1.3 | Definitions of Cybersecurity | 15 |
| 2 | **Cybersecurity within the European Union (EU)** | 2.1 | Fostering Cybersecurity within the European Union | 31 |
| | | 2.2 | Legal Aspects of Cybersecurity | 14 |
| | | 2.3 | Overview on the Tendencies of Cybersecurity Landscape | 41 |
| 3 | **Cyber-attacks: Social Engineering and Phishing** | 3.1 | Introduction to Cyber-attacks | 20 |
| | | 3.2 | Social Engineering Modules and Manipulation | 73 |
| | | 3.3 | Different Types of Phishing Attacks and Techniques | 37 |
| | | 3.4 | Case Studies | 37 |
| 4 | **Overview of Understanding and Handling Cyber-attacks** | 4.1 | Basic Knowledge on e-Security | 22 |
| | | 4.2 | Proactive Actions | 59 |
| | | 4.3 | Recognising Phishing Attacks | 108 |
| | | 4.4 | Handling Cyber-attacks | 87 |
| | | 4.5 | Minimising Damage through Incident Response | 34 |
| | | | **Total:** | **649** |

*Table 3. Summary on learning material*

**Tasks in an online learning environment**

The content of the course can be viewed on-screen and/or downloaded in .pdf format. Once a registered participant has reviewed all the training material on a particular topic, he/she can test their knowledge by taking a self-test. Points will be awarded for this.

---

2 **CyberPhish Extended Curriculum**: https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2_Extended-version-of-curricula_EN.pdf

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

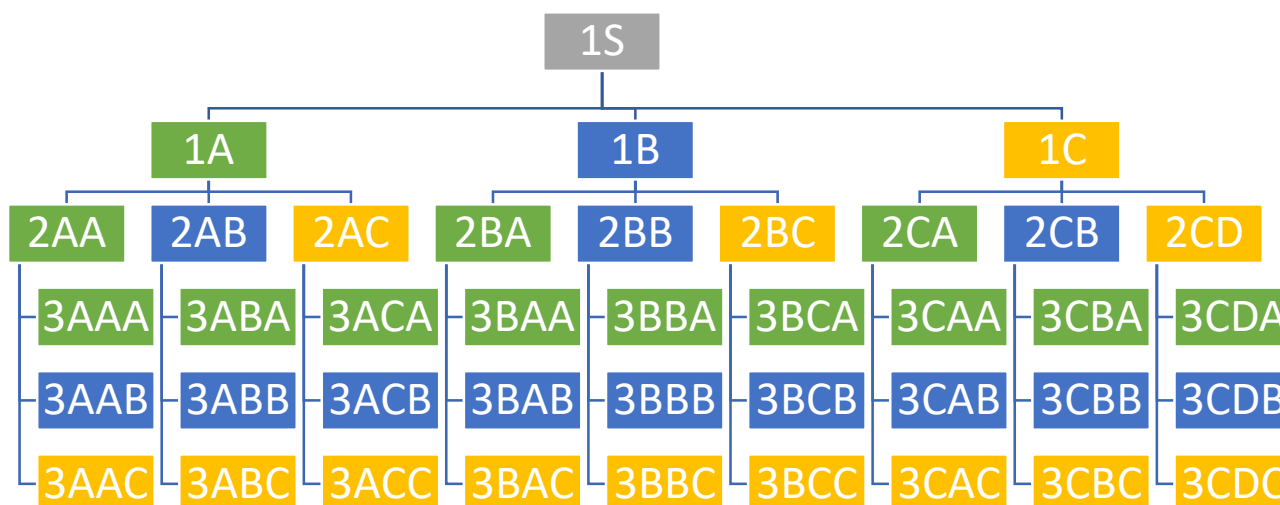*Figure 14. Self-evaluation test button in the course participant's environment*



*Figure 15. A fragment of Self-evaluating test*

**Simulations**

The simulation simulates actual fraud attacks by presenting the process to the user in a playful way. The simulation aims to help people improve their critical thinking about cyber security and fraud by recognising phishing, spam, cyber bullying and other incidents. The project partners developed 55 simulations.

A simulation consists of a description of the situation, the objective, the actors, the type of attack and several (3-4) response options for selecting the user's behaviour.

All simulations are based on a decision tree approach. Figure 15 shows the simulation model. Each simulation has three levels. The total number of options (possible choices) shall be at least 50, with a maximum of 84 options.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

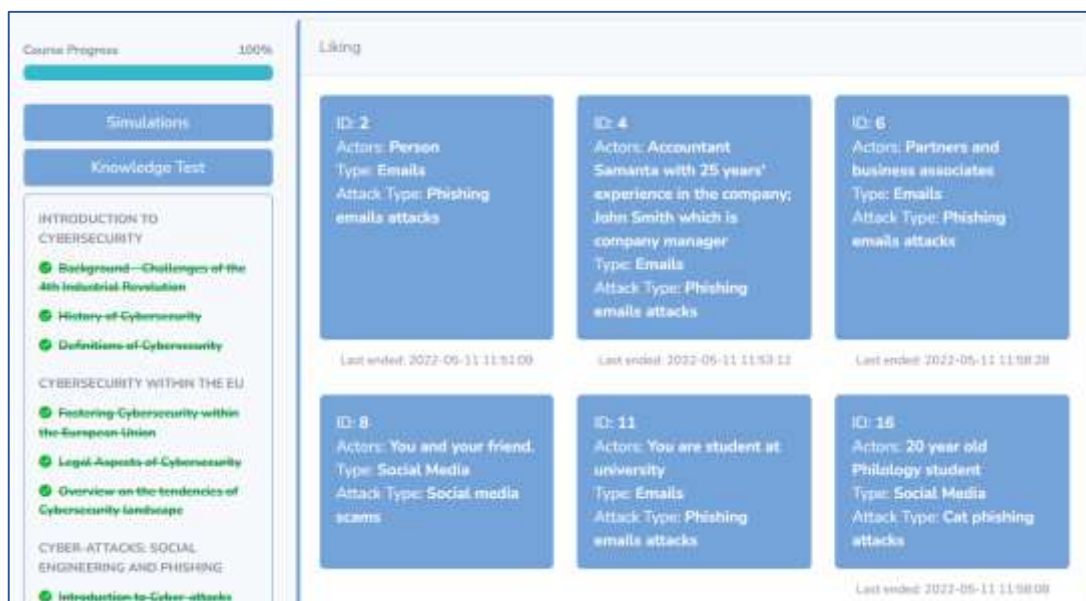*Figure 16. The simulation model is based on a decision tree approach*

In the simulation, each answer chosen by the user leads to the next level of possible answer choices. The simulation has three types of solutions: correct, partially correct and incorrect. For each answer, the system awards a certain number of points to the course participant. The system provides feedback on the screen if a partially correct or incorrect answer is selected. Suggestions are also given as to which part of the material the student should repeat and which topic they should look into further.

The participant can select simulations by topic/category.
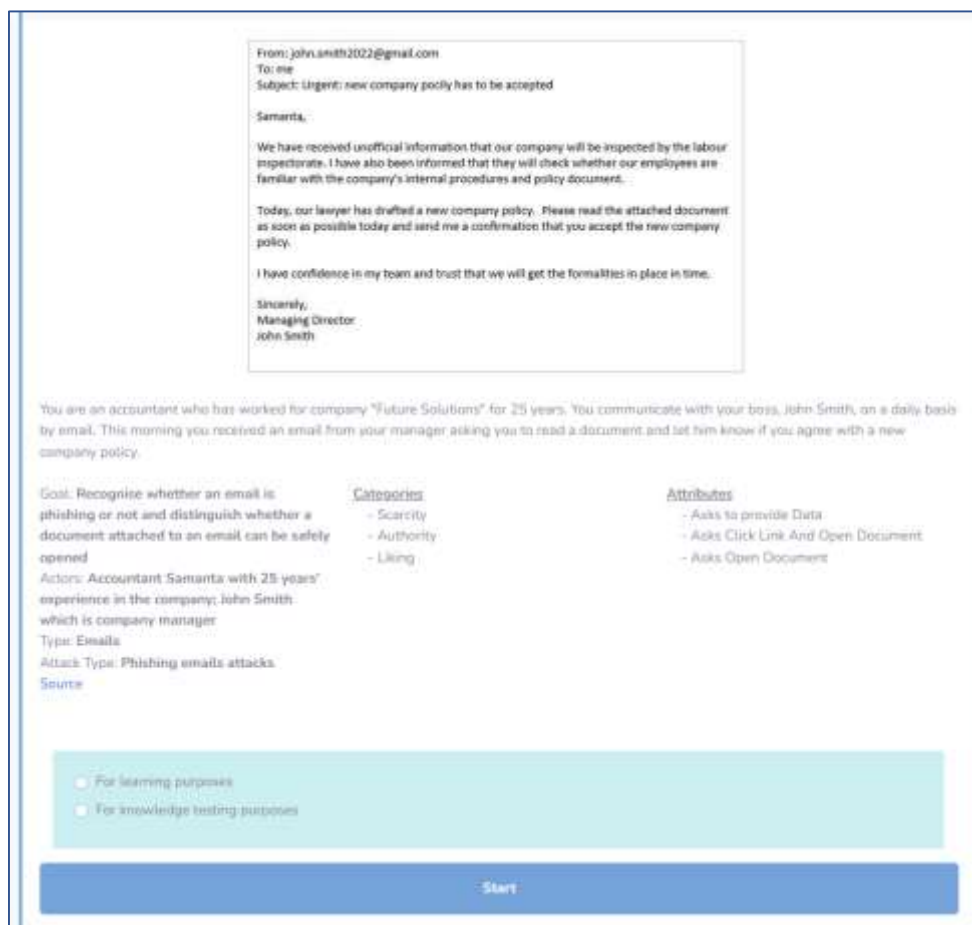


*Figure 17. Simulation categories/topics*

Simulations can be used in two ways: for learning and to test knowledge. In one way, feedback is given to the trainee after each situation, and in the other, feedback is given only after the entire simulation scenario has been completed. Points are awarded for solving the simulations, and a badge is awarded for solving all scenarios.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

*Figure 18. Choice of simulations in the Liking topic*

After selecting a simulation, the course participant is shown a description of the situation, the purpose of the simulation, the characters, the type of phishing attack and other attributes. Often (but not always), a picture is shown to enhance the impression (to make the participant more empathetic).

There is then the possibility to choose the purpose of the simulation: for learning purposes or to test knowledge.



*Figure 19. Example of a simulation solution*

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

Once the simulation has started, the participant is presented with choices. They have to choose how he/she would behave in such a situation. The figure below shows an example of a simulation solution.
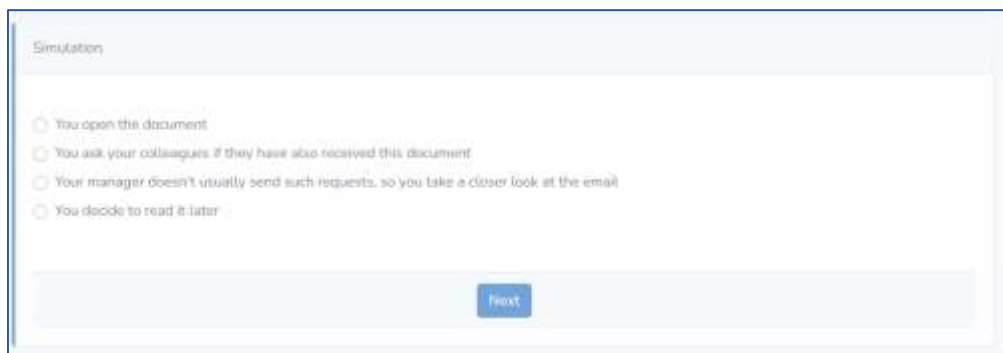


*Figure 20. A simulation solution*

During the simulation, the user receives on-screen feedback when an incorrect or partially correct answer is selected. Figure 21 illustrates On-screen feedback to the user during the simulation solution.
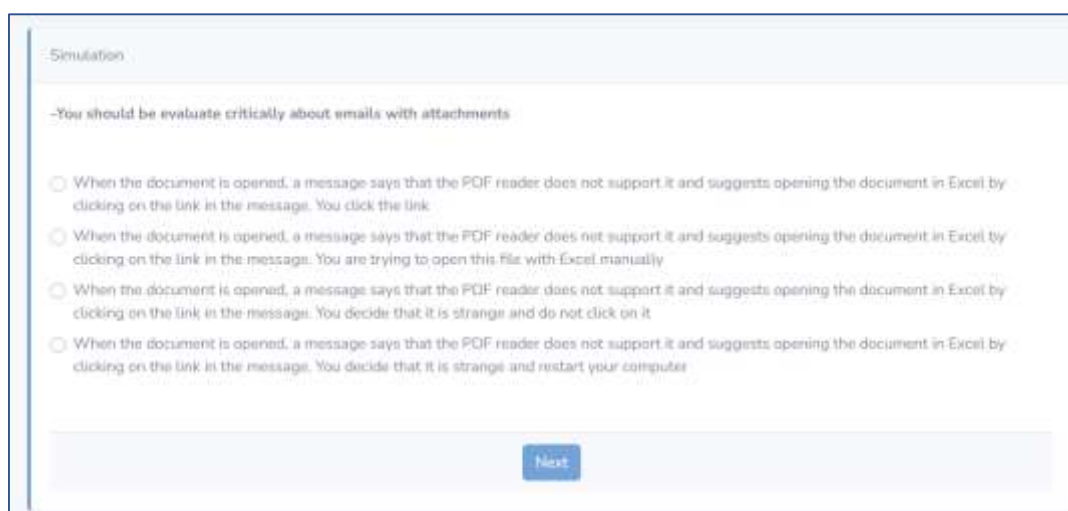


*Figure 21. On-screen feedback to the user during the simulation solution*

When the simulation is complete, the user is presented with a message showing the number of points scored and inviting them to solve other simulations. If the simulation was solved incorrectly, a recommendation to solve the simulation again is given (see Figure 21).
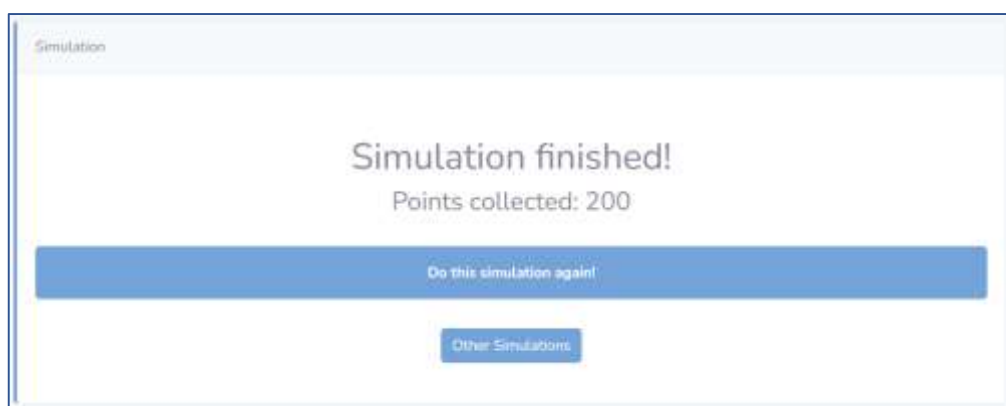


*Figure 22. Window of Completed simulation*

**Knowledge Evaluation Test**

After studying the training material (self-tests and simulations), the participant is presented with a button in the learning environment to take a knowledge test. During the pilot training, the knowledge test can be taken three times.
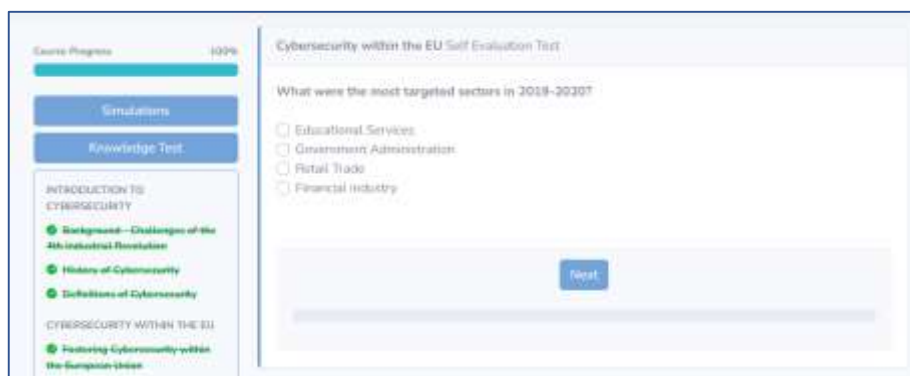


*Figure 23. Example of Knowledge evaluation test question*

At the end of the knowledge test, the course participant sees a percentage of their knowledge assessment.
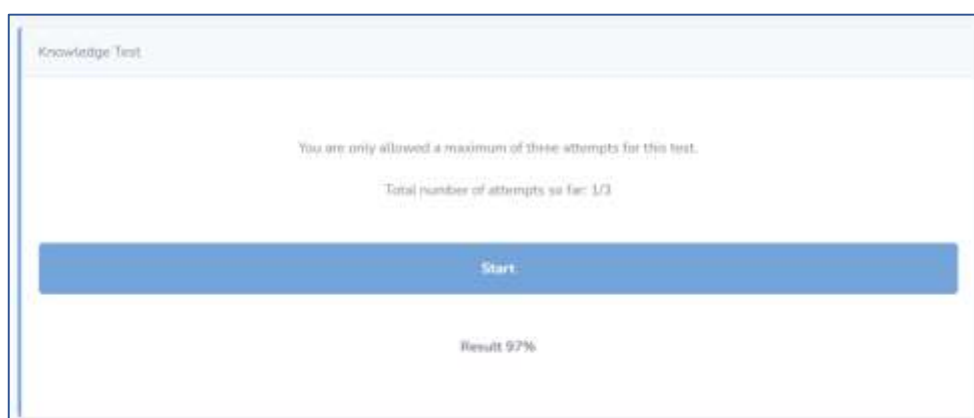


*Figure 24. Example of the assessment window for the Knowledge evaluation test*

*Note:* The knowledge test is designed to assess knowledge. This test is not intended for learning purposes. Knowledge tests are not publicly disclosed to participants, mentors and/or teachers. The questions are available in text format to all project partners/developers and the system does not provide access to the detailed test results. Other mentors/teachers will also be unable to view the full test results.

**Knowledge tests**

The partners have agreed to develop the questions for the self-tests and the questions for the knowledge tests based on the information provided in the application. The questions will be of the following several types.

There will be three types of questions in the **self-evaluation tests**:

- multiple-choice questions with one correct answer (number of possible answers: 3-6),

- multiple-choice questions (4-6 possible answers),

- yes/No questions.

The partners have agreed/decided on the amount of questions/quantity of questions per topic of the learning material. For example, 8-14 questions from the topics "Introduction to Cyber Security" and "Overview of Cyber Security in the EU". Create 12-20 questions each from the topics "Cyber-attacks - social engineering and phishing" and "Understanding and managing cyber-attacks".
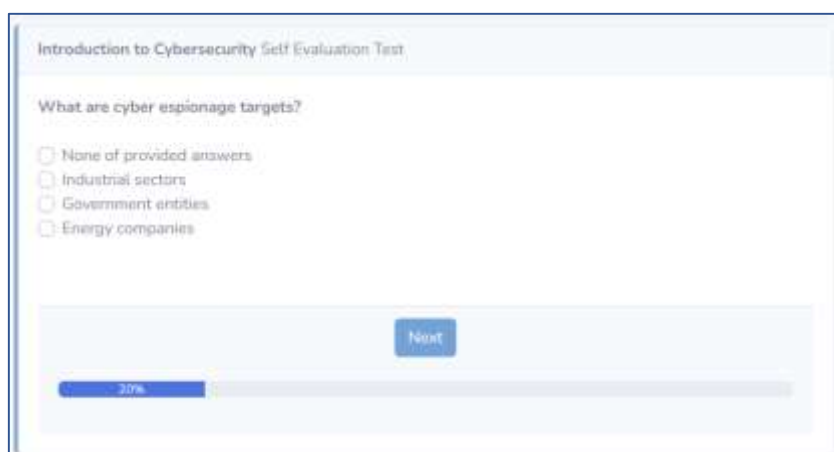
Specification for Self-evaluation questions:

| Modules | Self-evaluation questions developed |
|---|---|
| Introduction to cyber security | 13 |
| Overview of cyber security in the EU | 12 |
| Cyber-attacks - social engineering and phishing | 16 |
| Understanding and managing cyber-attacks | 19 |
| **Total:** | **60** |

*Table 4. Specification of self-evaluation test questions*

A button "Self-Evaluation test" appears in the learning environment when all sub-topics in a particular module are reviewed. A test consists of five questions. The questions are randomly selected from the current category question bank.

A progress bar is displayed at the bottom of the screen during the Self-Evaluation test, showing the percentage of questions answered and the number of questions remaining.



*Figure 25. An example of the Self-Evaluation test question in the category "Introduction to Cybersecurity"*

At the end of the Self-Evaluation test, the correct and incorrect answers are shown to the participant. Answers marked by the trainee are highlighted in green. Participant sees the start date and time, the end date and time as well as the number of points scored at the top right side of the screen.

There is no limit to the number of Self-Evaluation tests. The course participants can take it as often as they wish. The next time they take the test, they will be presented with other questions chosen at random.

Participants are also awarded a badge according to a rule agreed by the partners.

*Figure 26. Example of self-test results*

**Knowledge tests**. The partners have also agreed on the number of questions to be asked in the Knowledge Tests.

- All questions will have four answers, only one of which will be correct.

- Create 144 knowledge test questions.

The knowledge test will consist of a set of 36 questions. The test will take up to 45 minutes to complete. The pass rate will be 75 %.

The partners have agreed on the number of questions for each topic of the learning material. For example, 20-25 questions from the topics "Introduction to Cyber Security" and "Overview of Cyber Security in the EU". Develop 45-65 questions each on the topics "Cyber-attacks - social engineering and phishing" and "Understanding and managing cyber-attacks".

Specification of questions for knowledge assessment tests**:**

| Modules | Knowledge test questions developed |
|---|---|
| Introduction to cyber security | 24 |
| Overview of cyber security in the EU | 20 |
| Cyber-attacks - social engineering and phishing | 62 |
| Understanding and managing cyber-attacks | 46 |
| **Total:** | **152** |

*Table 5. Specification of questions for knowledge assessment tests*

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

The number of knowledge tests was limited during the pilot training. The maximum number of times this test can be taken is 3.

In the learning environment, the knowledge test button is displayed when the entire course is completed. Clicking the test button shows the number of attempts the participant will make to complete the test. If the test has been taken before, the result of the previous test is shown as a percentage.
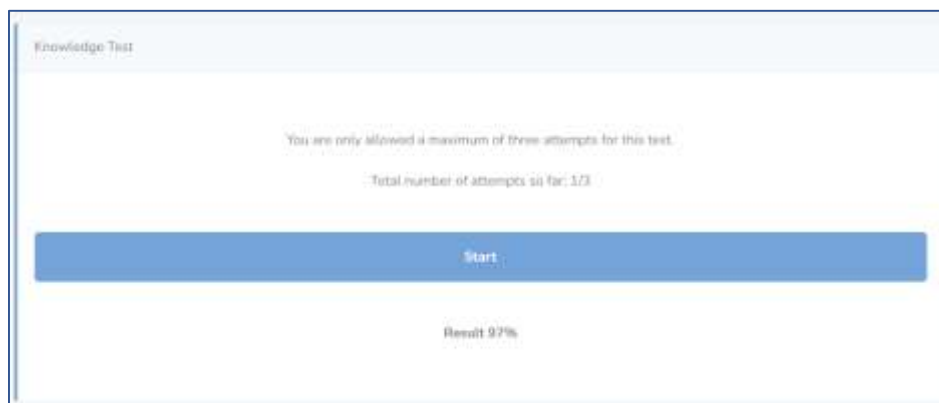


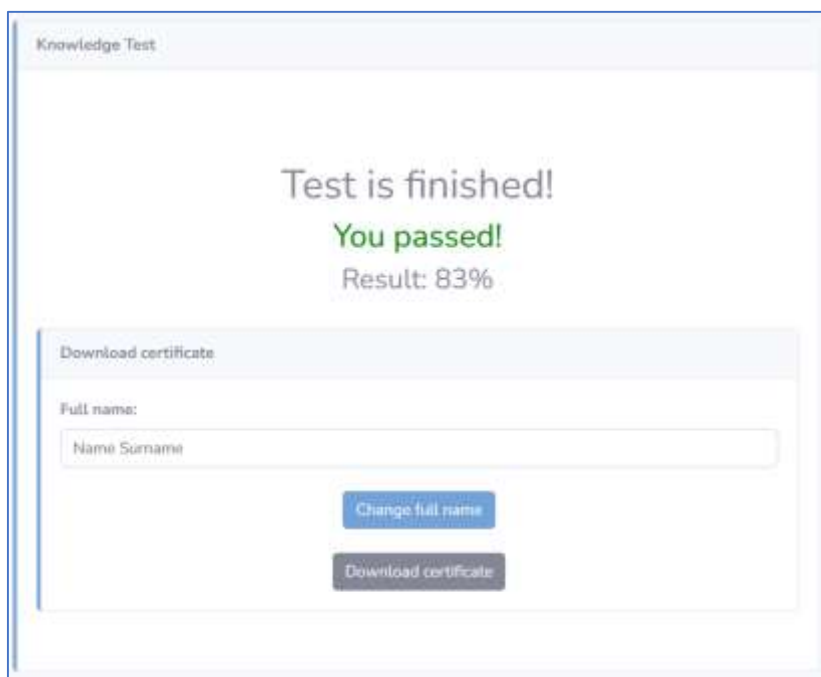*Figure 27. Knowledge test start window*

The knowledge test consists of a random selection of 36 questions. A rule is set for the number of questions to be randomly selected from each category. During the test, a progress bar shows the percentage of questions answered and the number of questions remaining. At the end of the test, the test score is displayed, but the participant cannot see how they have answered the questions as this is a knowledge assessment test.
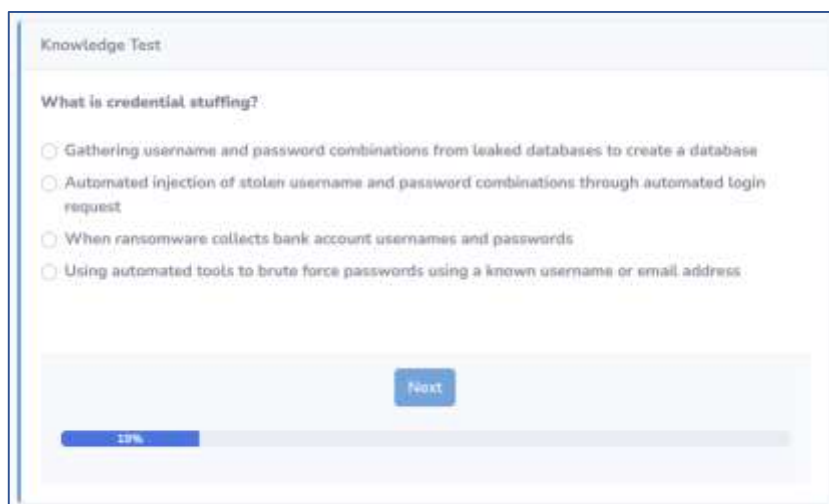


*Figure 28. Example of Knowledge test question*

If participants fail the test, they can try to repeat the training material, take the self-assessment tests, and try again to pass the knowledge test.

If successful, the participant is given the opportunity to enter his/her name and download the certificate in .pdf format.

*Figure 29. Passed knowledge test window*

**Certificate**

After passing the test, the participant receives a link to complete a post-test questionnaire, after which they can fill in their name and download the certificate in PDF format. This method of issuing the certificate facilitates the process of issuing the certificate.
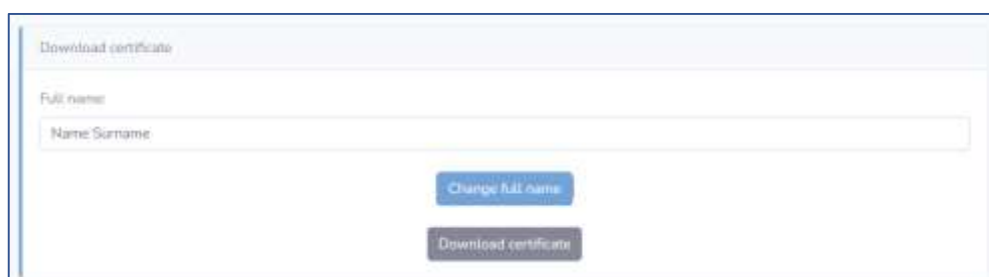


*Figure 30. Certificate generation window*

**Participants completed the training**

The Figure below shows the results of the training course. One hundred seventy-five participants completed (175) the training course and received a certificate: 36 in Estonia, 25 in Latvia, 26 in Cyprus, 30 in Malta and 58 in Lithuania. A further 17 participants completed the course without a certificate, i.e. their knowledge test score was below 75%.

**Participants who have completed the training**
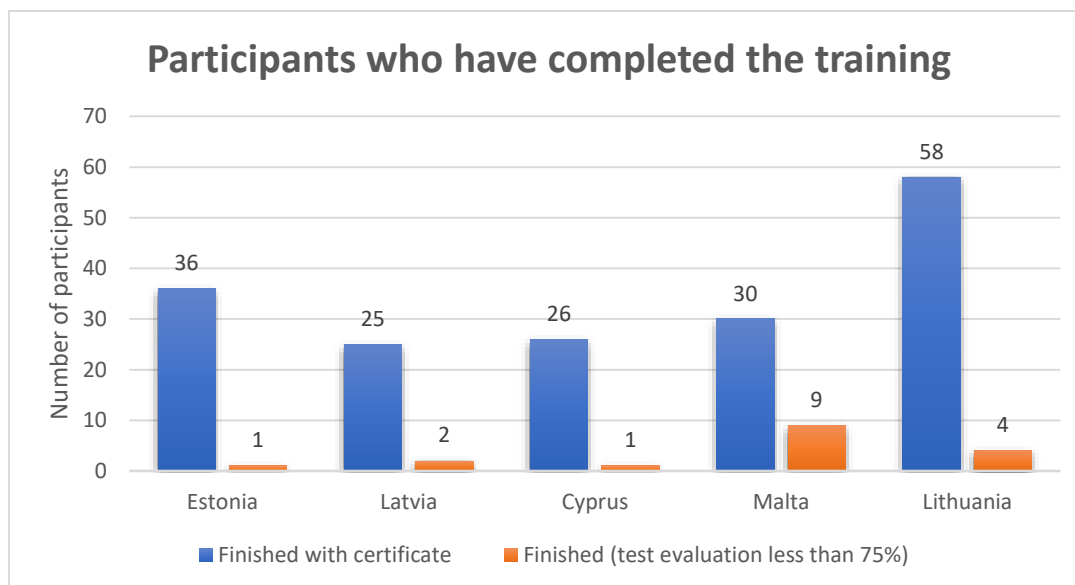
*Figure 31. Statistics on users who have completed the training*

The post-training questionnaires were completed and submitted by 139 participants: 31 in Estonia, 24 in Latvia, 16 in Cyprus, 27 in Malta and 40 in Lithuania.
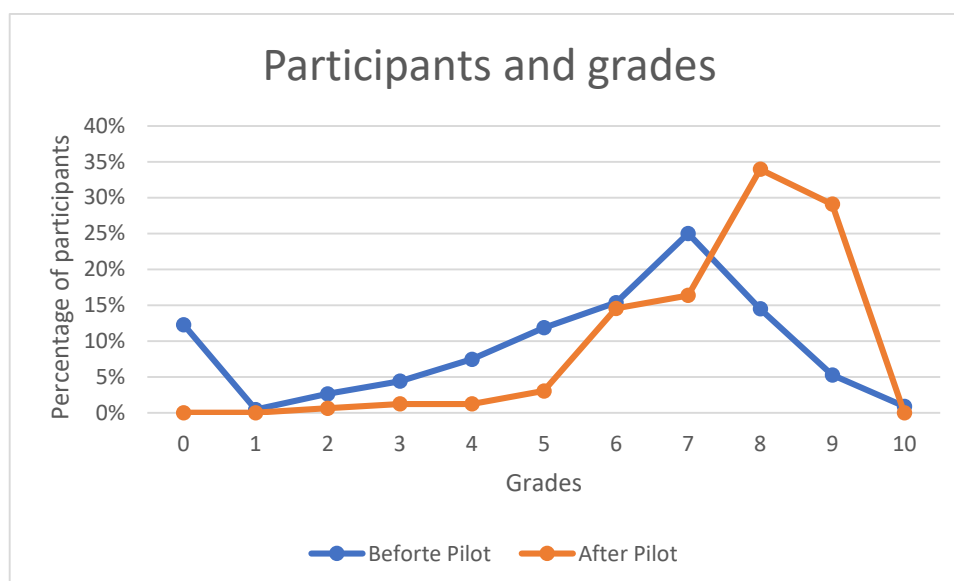
The post-training questionnaires were completed by 8 teachers: 2 in Malta, 3 in Lithuania and 1 each in Estonia, Latvia and Cyprus. Teachers agreed that the course achieved its goal of introducing cybersecurity and phishing to students (the same percentage of respondents indicated that they agree and that strongly agree with the statement). Respondents agree (62.5%) and strongly agree (37.5%) that the amount of detail was provided for the topics covered by the programme was appropriate. Majority of teachers (62.5%) strongly agree with statements "The time provided for participants to complete the pilot course was sufficient" and "Areas of topics covered by the course were appropriate for the target audience".

Teachers commented that the course is well designed and develops participants' awareness and critical thinking. Its introduction should not be limited to ICT related courses but should be introduced into different courses, either in part or in full. The most positive feedback comes from the scenario solutions.

**Comparison of participants' knowledge before and after pilot training**

Comparing the pre- and post-training knowledge assessment showed that participants significantly improved their knowledge of cyber security and phishing. The graph below shows how participants' knowledge of cyber security and fraud looked before and after the pilot training. The horizontal axis shows the ranges of scores (grades) and the vertical axis shows the percentage of students with the corresponding score.

Thus, the figure shows that after the CyberPhish training, the participants' performance improved significantly, i.e. more students obtained grades of 8 or higher. Meanwhile, the number of participants who failed the knowledge test, i.e. with a score between 0 and 6, decreased.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

*Figure 32. Participants' knowledge of cyber security and fishing before and after the pilot training*

## 6. PILOT TRAINING IN PARTNERS COUNTRIES

This chapter presents the experience of partner countries - Estonia, Cyprus, Latvia, Lithuania and Malta - of training programme implementation. Each country provides information related to areas including Participants' information and selection process, participants' profile, Student's motivation to join pilot training, training process organization, and participants' opinion on the content.

### Lithuania

**Participants' information and selection process**

To assess the quality of the CyberPhish course, the project partners have carried out pilot training in their countries. In Lithuania, the pilot training was carried out by inviting members of the VU Kaunas faculty community, mainly students. The invitations were posted on the Faculty's Facebook page, website, and lecturers presented the project during their lectures. The project partner, Information Technology Institute, prepared guidelines, developed questionnaires before and after the training, monitored the progress of the pilot training for all partners, and provided statistical information to the partners after the training data was systematized.

**Participants' profile**

The participants in the pilot training were 20-23 years old, and there were slightly more males than females, with 60% of the participants being males.

**Students 'motivation to join training pilot training**

The students were motivated by the fact that with the recent increase in cyber-attacks and theft of personal data, everyone must have a good knowledge of cyber security. Everyone should understand cyber hygiene, how phishing attacks work, and what social engineering is. All this increases our own resilience to cyber-criminals. That's why students were eager to join the Cyberphish distance learning course. Students who complete the course and receive a certificate are awarded an extra point towards their course grade. The course was a compulsory laboratory exercise for studying Information Systems and Cyber Security. Students were encouraged not only to familiarize themselves with the course material and to try out simulations but also to observe possible inaccuracies in the system and errors left behind. They were also rewarded for this activity.

**Training process organization**

The Lithuanian pilot training was attended by students from Economics and Management, Lithuanian Philology and Promotion, Applied Systems of Finance and Accounting, and Information Systems and Cyber Security. It was decided to

invite students from a wide range of study programmes to get as much feedback as possible, assessing not only the training material, the user-friendliness of the learning environment, but also the quality of the course. The project application foresaw inviting at least 24 participants in each partner country. Notably, the number of participants in the pilot training in Lithuania has been significantly higher, with more than 90 participants joining the CyberPhish course so far, 58 of whom have completed the course and have been issued with a course completion certificate.

**Participants' opinion on the content**

The main objective of the CyberPhish pilot training was to test and assess their knowledge about online fraud. It is encouraging that most participants in the pilot training in Lithuania were satisfied with the CyberPhish course. 43% of the participants stated that the simulations integrated in the CyberPhish course improved their ability to identify online fraud attacks, and a further 52% indicated that they improved their ability to identify online fraud attacks even a lot.

Between 40% and 60% of the participants who completed the course said they had learnt many new things. Participants were very optimistic about the following topics. They stated that they had learned a lot of new things: "Handling of Cyber-Attacks", "Legal aspects of Cyber Security", "Different types of Phishing Attacks and Techniques" and "Social Engineering Modules and Manipulation".

The feedback provided by the participants of the CyberPhish pilot training has confirmed the partners' ambition to contribute to developing cybersecurity skills and the forming of a safer society through the CyberPhish course.

# Estonia

**Participants' information and selection process**

Participants took the course "Principles of Secure Software Design" at the University of Tartu. The pilot was a part of the course. The participants were mainly students of the Cybersecurity curriculum jointly given at the University of Tartu (UT) and Tallinn University of Technology (TalTech). In addition, the pilot included a few Erasmus+ students, who were also taking the aforementioned course.

Selection: the pilot was included as a part of this course because of the following reasons:

1. Since Phishing is recently reported as the number 1 security risk in Estonia, future Cybersecurity specialists must be aware of this risk, would be ready to react and would be able to teach others of its impacts;

2. The participants' background is very suitable to pilot this type of course. They are young specialists both in cybersecurity and computer science and can to comment on the deficiencies of both the course contents and the developed software platform.

3. The course contents complemented the "Principles of Secure Software Design" material. Phishing is yet another type of attack. Thus, similar principles (like in other security risks) were illustrated through the given pilot lectures, scenarios and risk recognition.

**Participants' profile**

The average age of the participants in the pilot training was 31 years, with the oldest — 47 and the youngest — 22-year-old. Participant males were six time more than females (31 males and five females). All participants were 1st year Master's students of the Cybersecurity program, 2nd semester. There were an equal number of Estonians and participants, indicating other countries (18 participants each).

**Student 's motivation to join training pilot training**

The pilot was a part of the course "Principles of Secure Software Design. Students could earn up to 10 points on the course assessment (depending on the final knowledge test).

**Training process organisation**

The training was executed online. The initialisation lecture was given on the 5th of May. The rest was given as a self-study assignment. The students could email their questions and feedback or ask about the training during other course lectures.

**Participants' opinions on the content**

A survey of students after pilot training showed that all students improved their knowledge of Phishing. Especially the knowledge improvement was noticed in Legal Aspects of Cybersecurity, Handling Cyber-attacks, The tendencies of

Cybersecurity landscape, Types of Phishing attacks and Techniques, Social engineering, and Recognizing Phishing attacks. All participants were satisfied with their knowledge of cybersecurity subjects after finishing the CyberPhish course. Almost all students agreed that simulations helped to improve their skills in recognising phishing. All participants strongly agreed that the online approach was suitable for the course subject, that the amount of time given to complete the course was sufficient, and they would recommend this course to other people. The majority of students agreed that they had a clear understanding of the course objectives, that the course content covered the course objectives, and that support through the course was appropriate.

## Malta

**Participants' information and selection process**

Cyber phishing affects several areas and not just Information Technology. In this regard, students from different study programmes were targeted. MECB invited participating students from Higher Education Institutions (HEI) through its social partners. In the Pilot training students from the Malta College of Arts, Science and Technology (MCAST) which is the main Vocational Education and Training (VET) provider on the island and the University of Malta (UoM) – Junior College took part. In addition to students, MECB Ltd also focused on other stakeholders including but not limited to experts, policy makers and teachers. These were invited to participate through the MECB website. Training material, scenarios, self-evaluation, and knowledge evaluation tests developed during the CyberPhish project were also used to identify the stakeholders' knowledge level before and after the course.

Trainers and facilitators from the HEI and from MECB Ltd were also selected to give details about the CyberPhish project and monitor the pilot training. Before the pilot, the trainers were briefed about the overall CyberPhish project including but not limited to the study research (IO1), the CyberPhish Curriculum (IO2) and Course material (IO3) and the developed scenarios (IO4). In this way it was intended to create project awareness and enable the trainers to aid the stakeholders in any difficulties. Additionally, they were shown how to use e-platform, self-evaluation, and knowledge evaluation tests. Before the pilot a discussion and briefing the learning methods that could be used for effective work with stakeholders was also held. During this session, trainers were given methodological guidelines developed explicitly for trainers together with and other guidelines for students, which were distributed to the students at the beginning of the pilot training.

**Participants' profile**

Forty-three participants took part in the pilot training. More than two-thirds of the participants were men (71.4%) and almost one-third were women (28.6%).  Most participants were employees (60.7%), 21.4% were students and one-tenth (10.7%) were business people. The rest of the participants indicated that they were self-employed and others.

**Training process organisation**

In total three pilot training were held in Malta as follows:

1) Face-to-Face (students from the Institute of Business Management and Commerce (IBMC) at MCAST)
2) Online (students following Information Technology courses at the Junior College UoM)
3) Open Course (inviting all stakeholders, including learners, experts, policy makers and teachers)

In total 75 learners registered on the system, out of which 57% (43) fully completed the final course. Out of these, 67% attempted the simulations while 91% went for the Final Assessment. Thirty learners attempting the assessment managed to get 75% and over of the total score.

**Participants' opinions on the content**

A survey of participants after the pilot training showed that they improved their knowledge about phishing in all cybersecurity subjects of the CyberPhish course. Participants also noted that they had gained much new knowledge about fishing. All participants were satisfied with their knowledge of cybersecurity subjects after finishing the CyberPhish course. Almost all students agreed that simulations helped to improve their skills recognizing phishing. Majority of respondents agreed or strongly agreed with statements:

- the amount of time given to complete the course to be ample;
- the training and support throughout the course to be appropriate;
- they had a clear understanding of the course objectives;
- the course content covered the course objectives;
- the online approach to learning was suitable for the course;

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

- they would recommend this course to other people.

# Cyprus

**Participants' information and selection process**

During the pilot training in Cyprus, students from different study programmes were targeted – namely, IT studies, European studies, Marketing studies and so on. DOREA also has invited organisations (other adult education institutions as well as SMEs and their employees from our network) to take part in the pilot course.

DOREA has made an open call and invited everyone interested to join the pilot course considering that every person has to have these skills, not only the students of IT programmes. The invitations were done by email, phone calls and face-to-face meetings.

**Participants' profile**

Twenty-six participants took part in the pilot training. Majority of the participants were students in their 20s (92.3%) and the rest 7.7% were employees. More than two-thirds of the participants were women (76.9%) and almost one-third were men (23.1%).

**Training process organization**

The training in Cyprus was mostly organised online with online feedback/assistance from the trainer. On some occasions face to face consultations also took place.

For the online training each participant, who expressed interest to take part, received an email with the instructions and steps to be taken in order to register for the course. All students were invited to complete the self-evaluation test prior to registering for the course and after they have attended the course.

During the course, the trainer consulted the participants over emails, calls, and online and face-to-face meetings (when possible), guiding them, answering their questions, or providing additional information resources.

Most of the participants attended the course as they were generally interested in the topic and others have explained that they believe a certificate received will be useful in the future. Twenty-five of 26 participants have fully completed the course and received certificates.

**Participants' opinion on the content**

All participants indicated that they have gained a lot of new knowledge or improved their knowledge in all areas. Majority of participants have indicated that they especially gained a lot of new knowledge in "Social Engineering" and "Types of Phishing Attacks and Techniques". Majority of participants have improved their knowledge in "Legal aspects of Cybersecurity", "Proactive actions of cyber incidents" and "Handling Cyber Incidents". Only one participant had indicated that he had not learned anything new when it came to "Recognising Phishing Attacks".

Majority of participants indicated that they are satisfied with their own knowledge on cybersecurity subjects taught in the course after completing it. Some small percentage of participants (ranging from 3,8% to 11,5 %) were neutral when evaluating their knowledge. This may indicate that while they have believed they gained a lot of knowledge, there is still an area for improvement. Majority of participants have indicated that simulations either "strongly helped" or "helped" them to understand the cyber subjects taught. Majority of participants had great experience with the course in terms of understanding the course objectives, finding online approach and contents appropriate, having enough time to complete the course, etc. One1 participant did indicate that he did not find the online approach to learning was suitable for the course, one participant found the platform difficult to use and one person would not recommend this course to other people.

The trainer of the CyberPhish states that the course is very informative and covers all major topics that are necessary for students to understand the cybersecurity issues, phishing in particular, as well as learn how to protect oneself. She emphasized that the course is definitely useful not only for IT students to refresh their skills and knowledge but also for students from other areas, employees, and general society.

# Latvia

**Participants' information and selection process**

Pilot training was implemented with the social partners Riga Technical University (RTU) and Latvian Culture College, Therefore, students of these HEI were invited to participate. Altacom organized separate meetings with RTU and LKK student governments in order to present the CyberPhish project and the foreseen Pilot training. Students after the meeting were directed to the person in charge of non-formal education at their HEI's. Social partners and contacts from Latvian culture college, sent out invitations to students (mostly from non-IT faculties).

**Participants' profile**

Twenty-seven participants took part in the pilot training. The average age of the participants in the pilot training was 23 years, with the oldest — 26 and the youngest — 19-year-old. Participant males were one and half times more than females (60% males and 40% females). In general, participants were students from technical and cultural fields. Most of the participants were Latvians who are living in Riga currently, but there are also exchange students who were from different countries studying in Latvia.

**Students' motivation to join pilot training**

The pilot was introduced as s new additional non-formal education means which can help students gain valuable theoretical and practical skills in cyber security. Nowadays, those skills are very useful not only for personal use but also in almost all workplaces where computers are used. Therefore, some of the invited students decided that participation in the Pilot can be really beneficial for them and agreed to join.

**Training process organization**

The main information about the Pilot has been provided during the meeting with the student governments of RTU and LKK and in the invitation. In addition, participants could contact directly with their questions and feedback by email or other contacts (ex. Message on a social network).

There were 45 registered participants on the learning platform. 25 participants passed the knowledge test with scores above 75%. 2 participants passed the knowledge test (in Latvian) with scores below 75%

**Participants' opinion on the content**

A survey of participants after the pilot training showed that they gained a lot of knowledge about phishing in almost all cybersecurity subjects of the CyberPhish course. Participants improved their knowledge about phishing in "Legal aspects of Cybersecurity", "the Tendencies of Cybersecurity", "Proactive actions of cybersecurity" and "Handling Cyber-attacks" modules. Majority of participants were satisfied with their knowledge of cybersecurity subjects after finishing the CyberPhish course, especially with modules "Cyber-attacks – Social Engineering and Phishing" and "Understanding and Handling Cyber-attacks". Almost all students agreed that simulations helped to improve their skills recognizing phishing. Majority of respondents agreed or strongly agreed with statements:

- they would recommend this course to other people
- the training and support throughout the course to be appropriate;
- the online learning platform was easy to use;
- the amount of time given to complete the course to be ample;
- the course content covered the course objectives;
- they had a clear understanding of the course objectives;
- the online approach to learning was suitable for the course.

# CONCLUSIONS

Based on a needs analysis, the consortium of partners has developed a training curriculum on cyber security, cyber-attacks, social engineering, with a particular focus on identifying and preventing phishing. The curriculum was designed for blended learning, but its structure makes it flexible and can be used for both distance and face-to-face training. The full training programme consists of 30 hours corresponding to 1 ECTS.

The curriculum is structured in four distinct parts (modules): Introduction to Cybersecurity; Overview of Cybersecurity within the EU; Cyber-attacks – Social Engineering and Phishing; Understanding and Handling Cyberattacks.

Partners consortium developed the online training material following CyberPhish Curriculum and according to the 4th Industrial Revolution needs. During the project partners created learning material which consist of slides, assessments, and links to external sources and videos. Developed learning material was well evaluated by independent experts.

The developed curricula, training materials and learning environment can be used for various target groups, for example, students, educators, university staff (community members), Adult centres, and the business sector (employers and employees).

The developed e-learning materials, blended learning environment and simulations were integrated in subjects at the participating Universities during Pilot training.

The developed training material, simulations, self-evaluation tests and knowledge evaluation tests help to enhance participants' critical thinking, and skills in cybersecurity to be applied in their professional practice. The course CyberPhish can be successfully used to organize training for other target groups, not only during the pilot training in participating countries, but also through adaptation in other European countries.

Comparing the pre- and post-training knowledge assessment showed that participants significantly improved their knowledge of cyber security and phishing. Data shows that the participants' performance improved significantly, i.e. more students obtained grades of 8 or higher.

One hundred seventy-five participants completed (175) the training course and received a certificate: 36 in Estonia, 25 in Latvia, 26 in Cyprus, 30 in Malta and 58 in Lithuania. A further 17 participants completed the course without a certificate, i.e. their knowledge test score was below 75%.

# REFERENCES

1. ENISA (2019): Cybersecurity skills development in the EU. European Union Agency for Security. December, 2019. URL: Cybersecurity Skills Development in the EU — ENISA (europa.eu) (accessed 09/08/2022)
2. Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy  (accessed 09/08/2022)
3. Good practices in innovation on Cybersecurity under the NCSS, November 19, 2019
4. IO1 A2: Results "Analysis of Existing Cybersecurity training programmes", 2021, URL: https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A2-Report_Analysis-of-existing-Cybersecurity-training-programmes_EN.pdf
5. Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor
6. European Union Agency for Cybersecurity (2020):  Phishing - ENISA threat landscape 2019-2020
7. IO1 A1 "RECOGNISING PHISHING AND SKILLS GAPS", 2021, URL: https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A1-Report_Recognising-Phishing-and-Skills-Gaps_EN.pdf
8. Robert B. Cialdini (2006) The Psychology of Persuasion. Harper Business, 336p. ISBN: 978-0061241895
9. NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433

# ANNEX 1

# CYBERPHISH LEARNING ENVIRONMENT
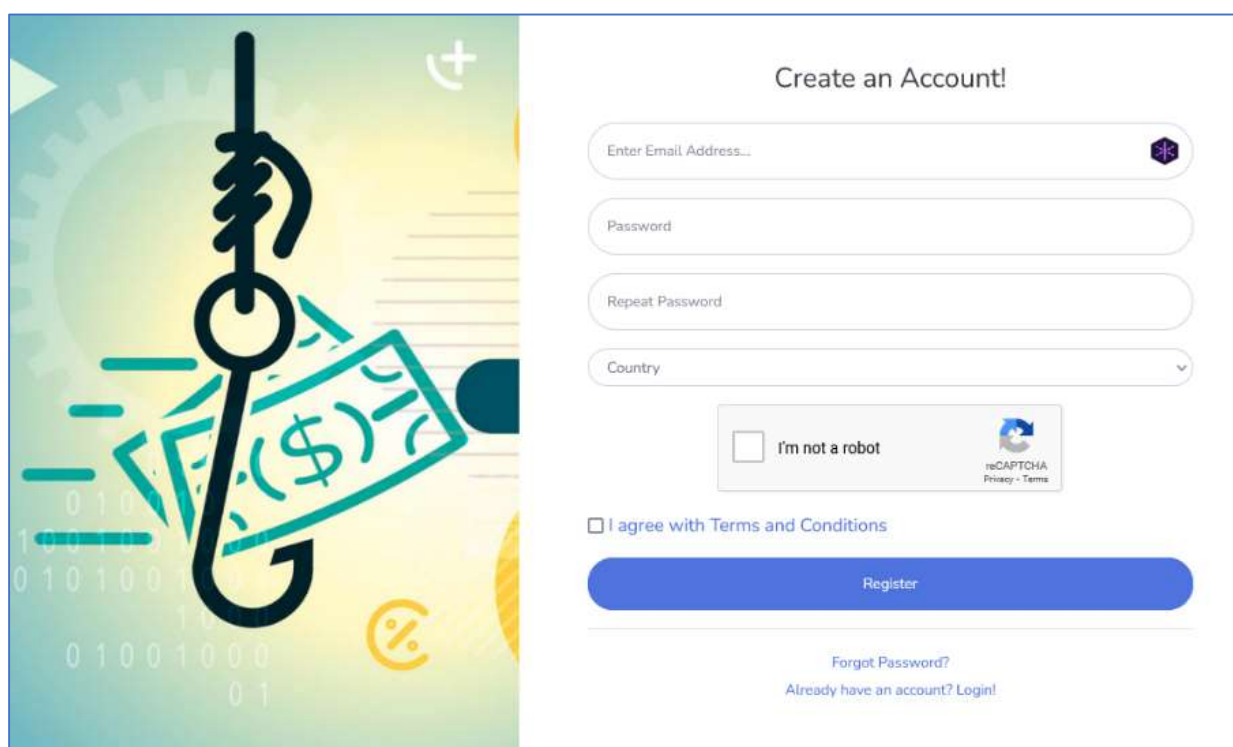
The learning materials hosted in the e-learning environment at https://cyberphish.vuknf.lt are available to all visitors and are free of charge. The study material is available in five languages: English, Estonian, Greek, Latvian and Lithuanian. Non-registered visitors can only view the learning material, but they cannot take self-tests, knowledge tests, earn and collect badges, run simulations, or receive certificates. To become a registered visitor to the website you need to register.

## Registration to the e-learning environment

To become a registered user, create an account by clicking the "Sign up" button.



After clicking **Sign up** at the top of the page type your email, password, repeat your password and select your country. You must also confirm that you are not a robot and that you accept the terms and conditions and then click **Register**.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future

A confirmation link will be sent to you by email once you have registered. Click on the link.

Note: If the student has not received the confirmation email from the system it is necessary to check the spam. It is possible that the confirmation email will end up in the spam/junk folder.

Create an Account!

User registered! Check your email for verification link.

Enter Email Address...

Password

Click the confirmation link to log in to the system.

Welcome Back!

Enter Email Address...

Password

Login

Forgot Password?

Create an Account!

## User account

Once you logged in, click on your email address at the top of the page and click **My Information** item.
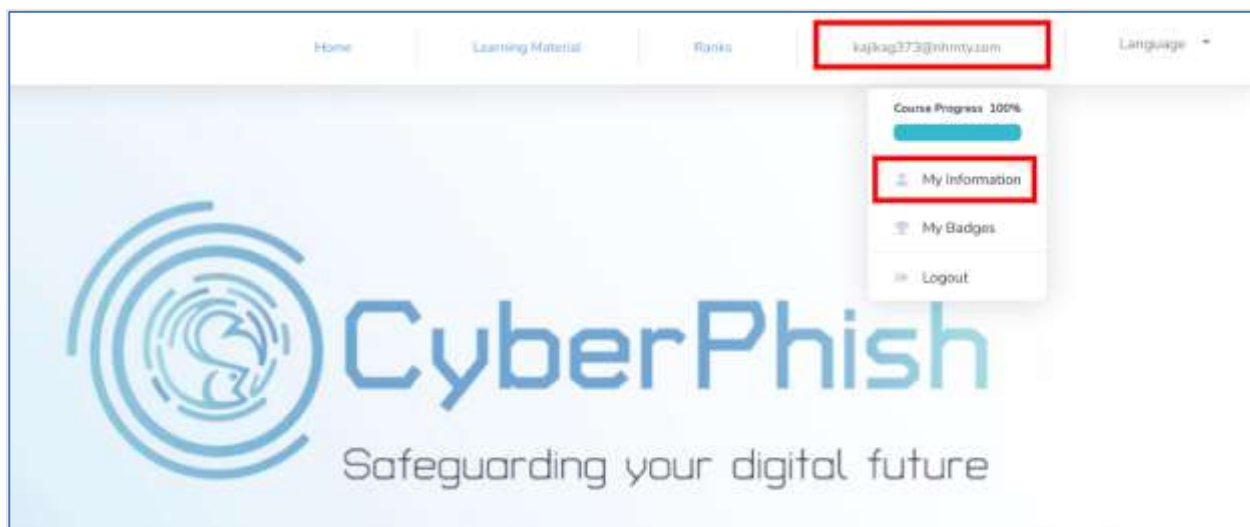
On the left side of **My Information** page, you will see the main user menu, which links to **My Information** page (your current page), My **Badges page**, **Self-Evaluation History** and **Simulations History** pages.

You can change your username and password on the **My Information** page.
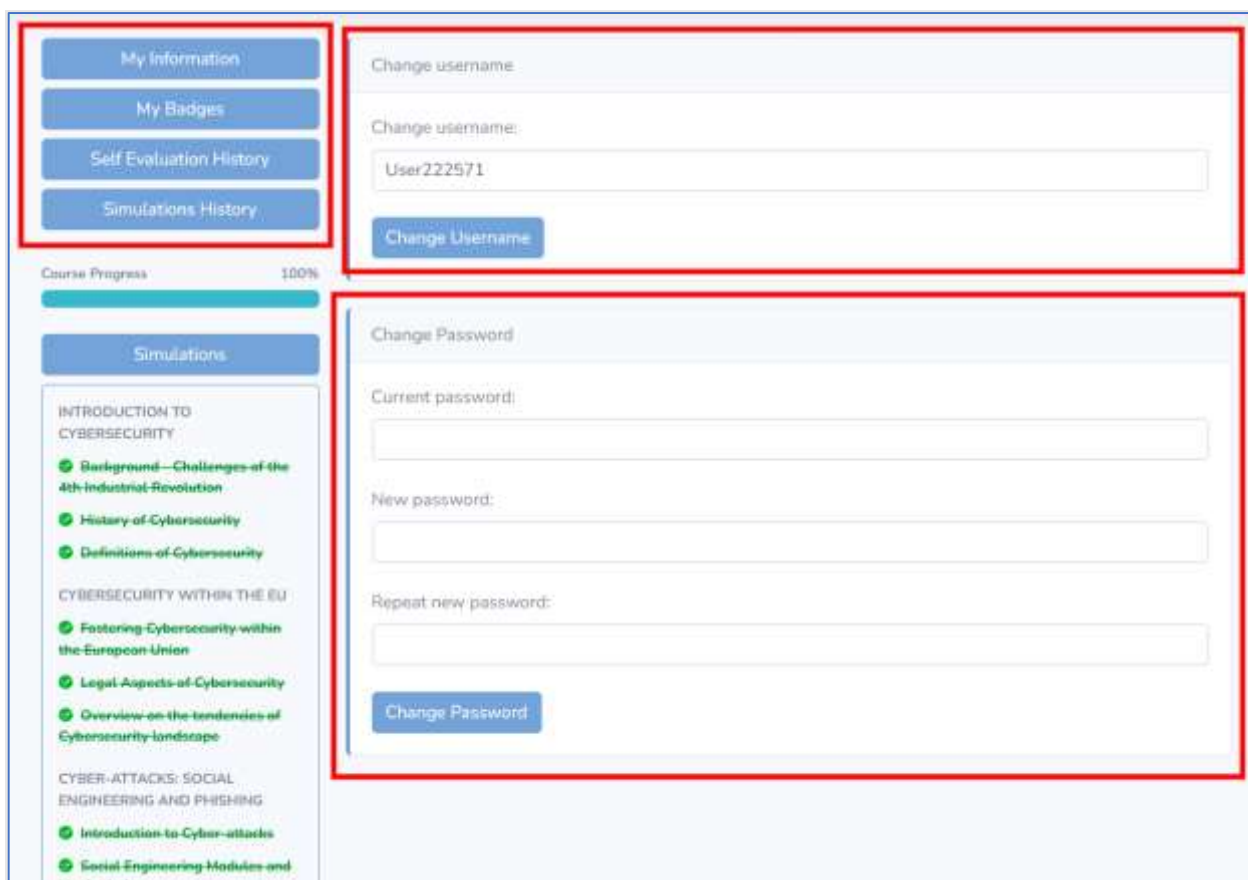


On **My Badges** page, you will see all the badges you have collected for the different tasks you have completed.
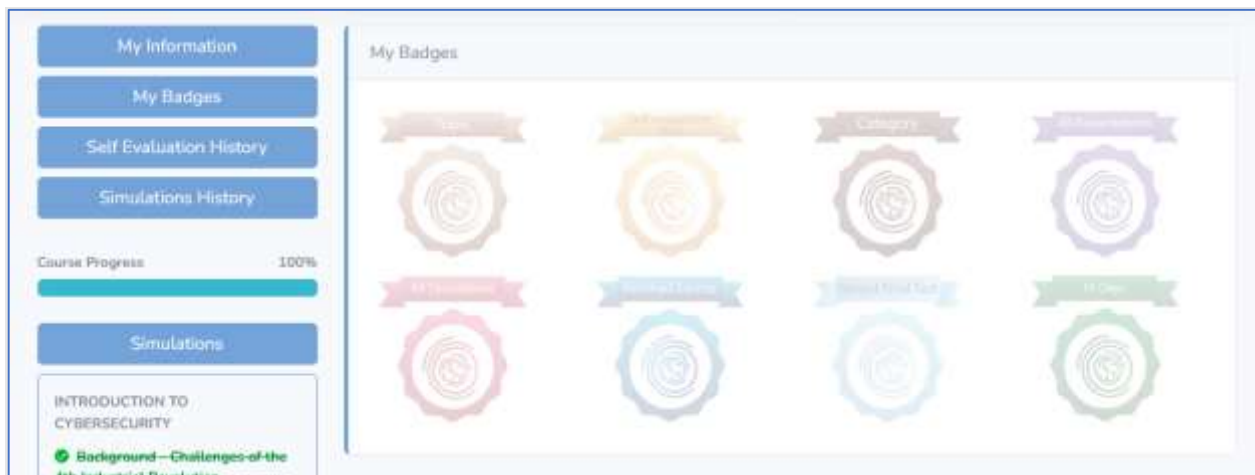
On the **Self Evaluation History** page, you will be able to see the history of all Self-Evaluation tests you started or completed. If Self-Evaluation test is incomplete, you can do it by clicking on the name of the test. If test is completed, you can click on it to see the results.



On the **Simulations History** page, you can view the history of simulations that you have been started or completed. If a simulation has not been completed, you can do it by clicking on the name of the simulation. If simulation is completed, you can see the results by clicking on it.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future
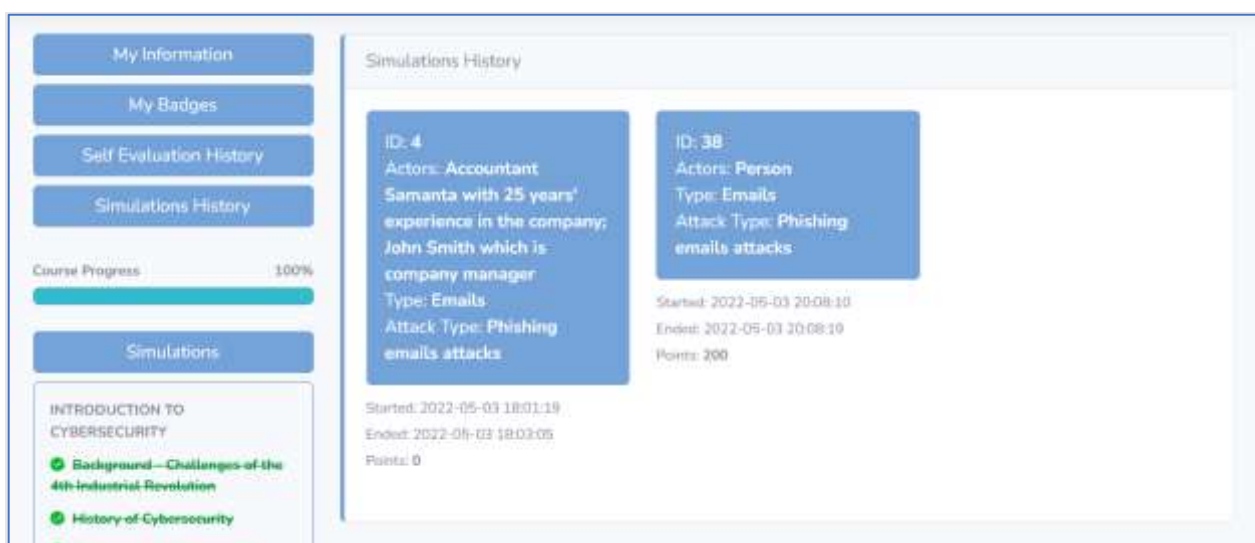
## Learning material

You can access the learning materials at the top of the page by selecting the **Learning Material** menu item and selecting the topic you are interested in\*.

*\*All leaning material can be accessed without registration, but some features may be limited. The trainee can read the training material without logging into the system, but they will not be able to confirm the viewing status of the training material, nor will they have access to the tests and simulations.*
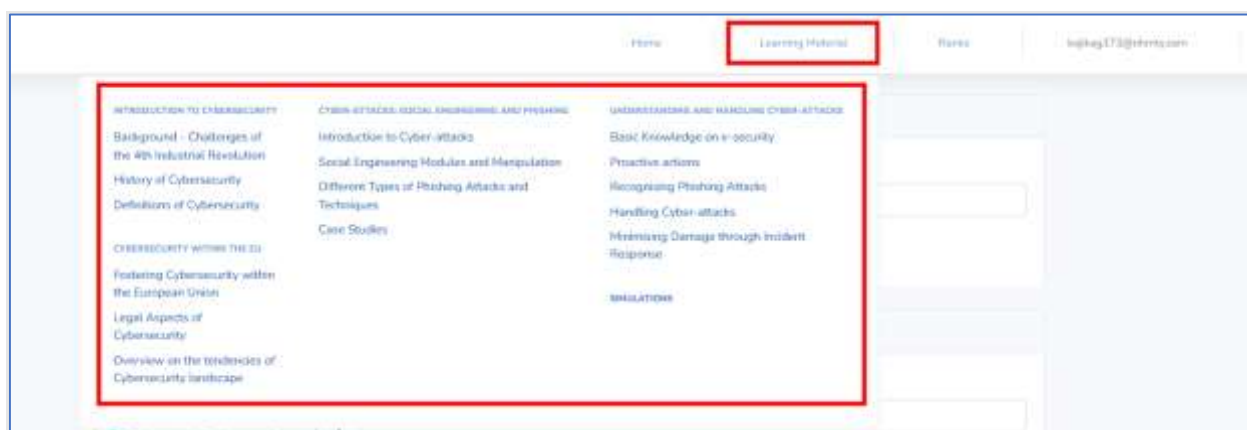


If you select any topic, you will see the slides for that topic on the main part of the page and links to all topic on the left side of the page. If you are logged in, you can mark topics as completed by pressing button **Mark as Completed!** on the right side of the top of the page and see the progress of your course on the left side of the page.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future
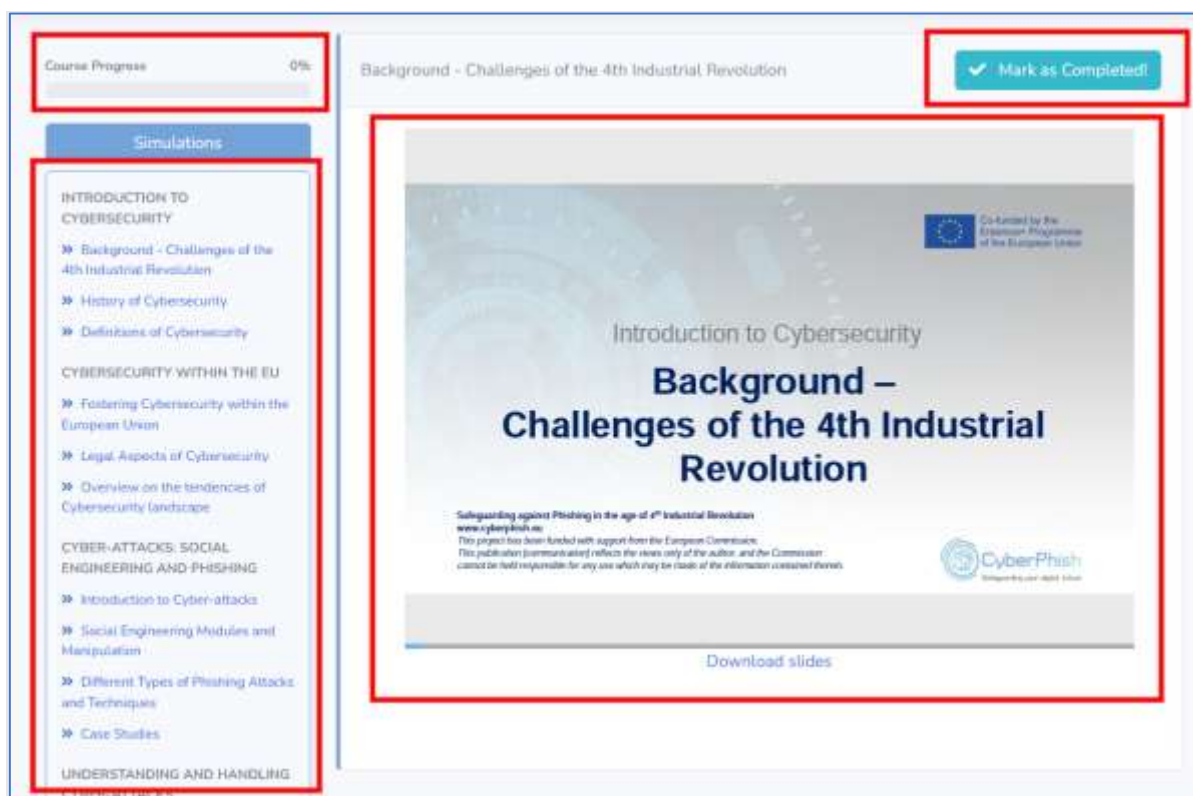
## Self-Evaluation test

To access Self Evaluation questions, you need mark each topic in the category as completed. You then will see the **Self Evaluation Test** button at the top of the main page. You must be logged in to access the **Self Evaluation Test**.



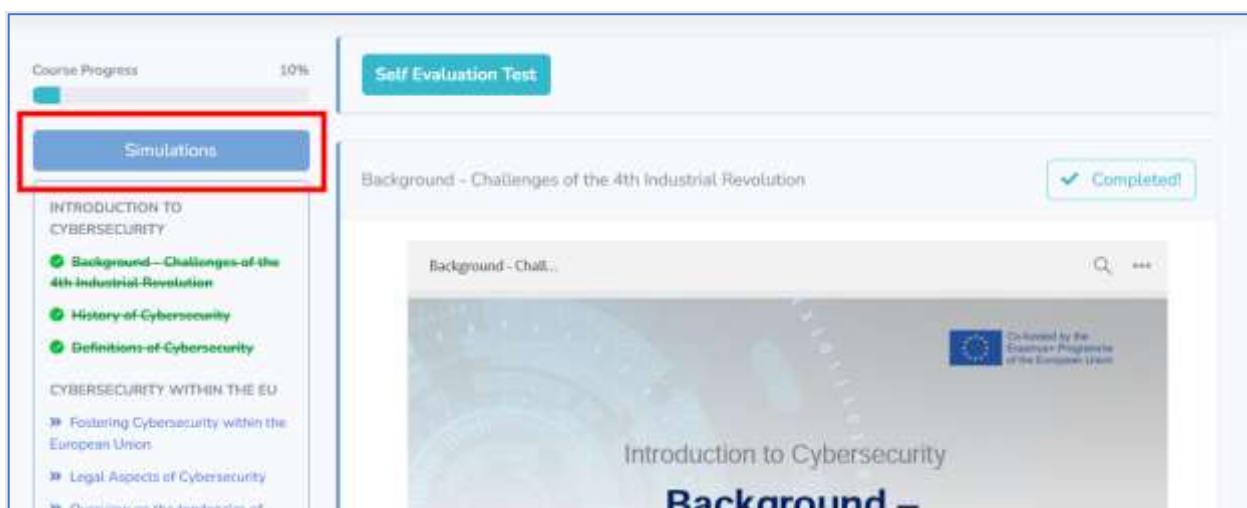If you click on the **Self Evaluation Test** button, you will receive 5 questions for that category to assess your knowledge.
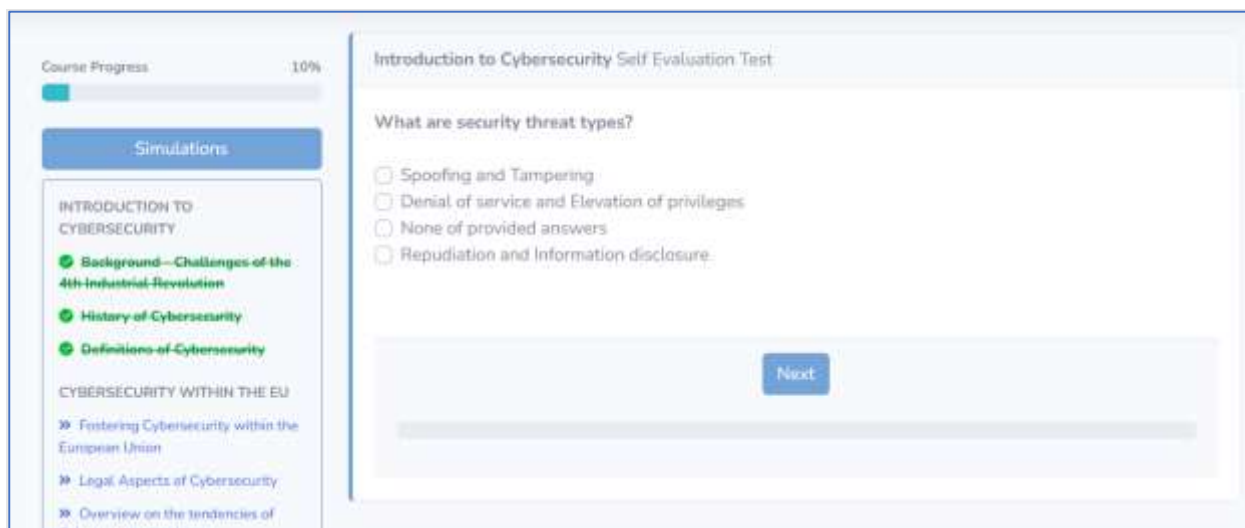


## Simulations

Users can only access simulations by logging in.

You can access simulations by clicking on the **Learning Material** and selecting **Simulations.**
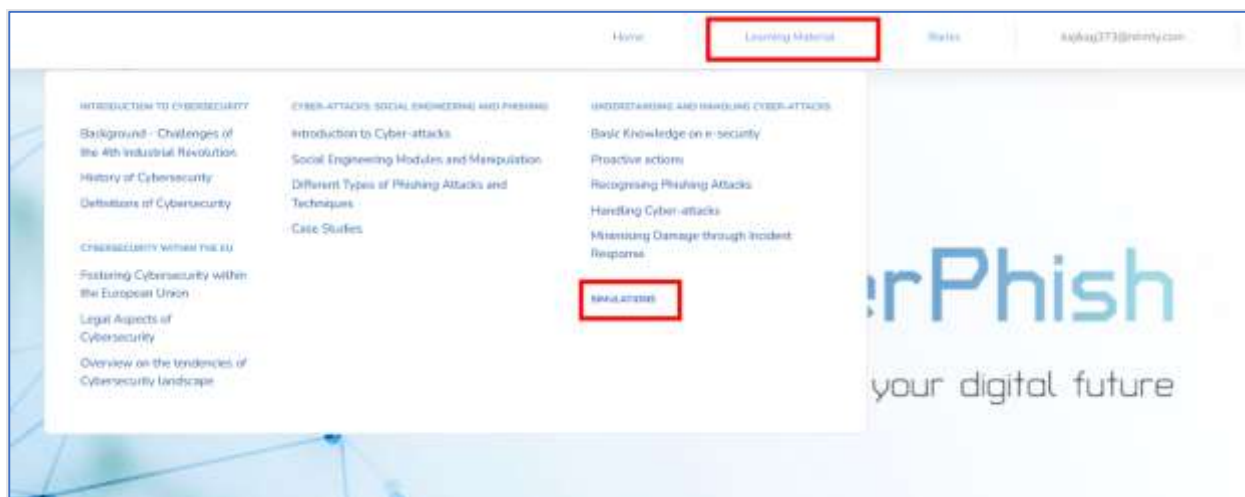
You can access simulations from any selected **Learning Material** topic page, too.



When you click **Simulations,** you have to select a category of simulations. A single simulation can be listed in several categories.
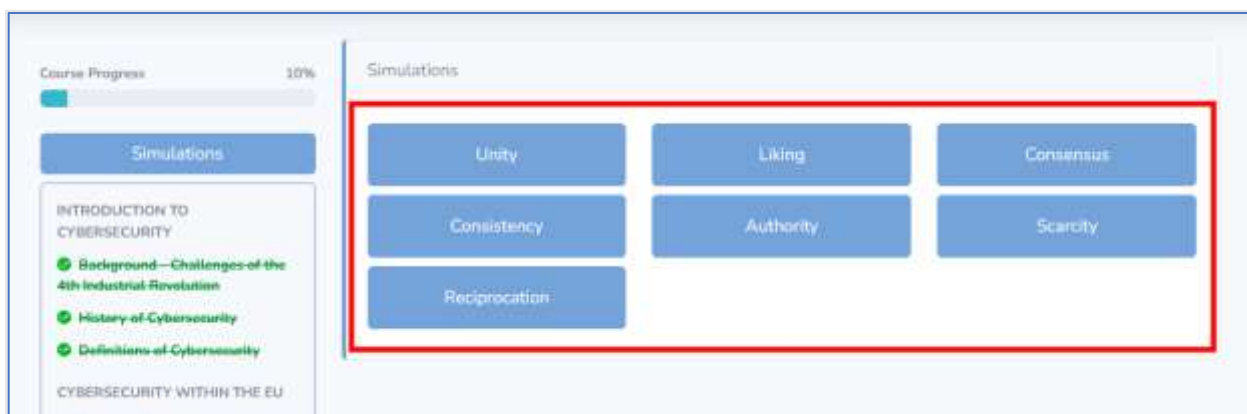


Selecting the Simulations category will allow you to select simulations in that category. If you have ever completed a particular simulation, you will see a timestamp under that simulation.

Funded by the
Erasmus+ Programme
of the European Union

CyberPhish
Safeguarding your digital future
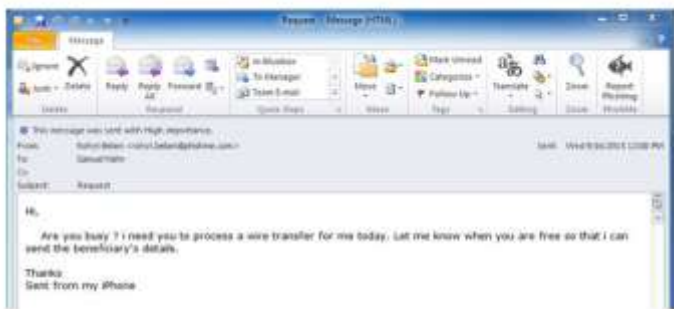
When you select any simulation, you see the description of the situation before you start solving it. Before you start, you have to choose whether you want to do it for **learning purposes** or **For knowledge testing purposes**.

If you choose **for learning purposes**, you will see the feedback after each answered question.

If you choose **for knowledge testing purposes**, you will see feedback only after you finish the simulation.

Click **Start**.

# User ranks

This option ranks users according to their best performance on **Self-Evaluation Tests** and **Simulations**. You can access the user ranks by clicking **Ranks** at the top of the page and selecting either **Self-evaluation** or **Simulations**.