

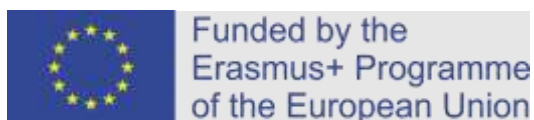
Safeguarding against Phishing in the age of 4 Industrial Revolution (CyberPhish)



A1: Methodological Guidelines for Trainers

Project Duration: November 2020 – November 2022

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



Funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission.

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Contents

| | |
|--|-----------|
| About the project | 3 |
| Guidelines on organizing training | 3 |
| Common procedures for training..... | 5 |
| Descriptions of how to work with e-platform | 9 |
| Working with innovative methods (i.e. simulation methods, lectures, seminars, practical trainings, Internet tools usage etc.) | 11 |
| Conclusions and recommendations | 12 |
| References..... | 13 |
| Annexes..... | 14 |
| Annex 1. Example of online invitation for to CyberPhish course..... | 14 |
| Annex 2. Example of a CyberPhish course completion certificate | 16 |
| Annex 3. Example of Post-course questionnaire for CyberPhish course participants | 17 |
| Annex 4. Example of Post-course questionnaire for CyberPhish course trainers, consultants and mentors..... | 23 |

ABOUT THE PROJECT

Fraud is one of the biggest problems recently, as cybercriminals use faster and more innovative technologies to carry out fraud campaigns. The development of human-powered phishing protection requires the education of users so that they can recognise and respond appropriately to phishing attacks.

The project aims to educate students of higher education institutions, educators, university staff (members of the community), education centres, and the business sector (employers and employees). In addition, the project also aims to encourage critical thinking of the target group in the field of cyber security.

The project team has developed a curriculum, e-learning material, a blended learning environment, self-evaluation tests, knowledge evaluation and assessment system, and game-based simulations for students and other users to protect against phishing attacks, as well as to build competences that will help them to be aware of the threats and to take proper preventive measures.

The main intellectual outputs are:

1. Study analysis and recommendations: Avoiding phishing attacks and improving critical thinking;
2. Course Curriculum;
3. Online learning material;
4. Simulations for education (gamification);
5. Self-evaluation and knowledge evaluation systems;
6. Methodological guidelines for trainers and implementation of the CyberPhish module.

GUIDELINES ON ORGANISING TRAINING

Suggestions and guidance on organizing training for participants of the CyberPhish module.

The Cyberphish course could be organised using a blended learning approach, combining online and face-to-face teaching methods. This means that the process of acquiring knowledge and skills is based on both face-to-face and online teaching: seminars led by a lecturer, independent work by participants using online learning materials, and group collaboration exercises.

It is important that participants could have the lecturer's support at any point of the learning process (except the final knowledge evaluation), i.e., could ask questions of interest, ask for help if they fail or do not understand how to do a task, and receive support and feedback from the lecturers.

Target group. Higher education students are the main target group of this project. During pilot training students were selected from different study programmes. They used advanced training material, practiced game-based simulations, and performed self-evaluation and knowledge evaluation tests to identify their knowledge level before and after the course. Participants must have basic digital literacy skills. Beside this there are no other prerequisites for students' knowledge or skills.

Teachers also have been able to access a modern course curriculum based on the latest research in the partner countries; e-learning materials developed by experts in their field, enriched with exercises for students, links to additional reading material (recent literature), and related video resources. Thus they update and improve their existing knowledge. Teachers could learn about innovative teaching and learning methods, such as self-tests and knowledge tests in an online environment, as well as simulations, which simulate real-life situations attractively and playfully.

Other beneficiaries affected by the project are educators, university staff, education centres and the business sector (employers and employees). They will also benefit by broadening and deepening their existing knowledge and competences, feeling safer online, avoiding sensitive/personal information leakage and avoiding financial losses, both personally and in their organisations.

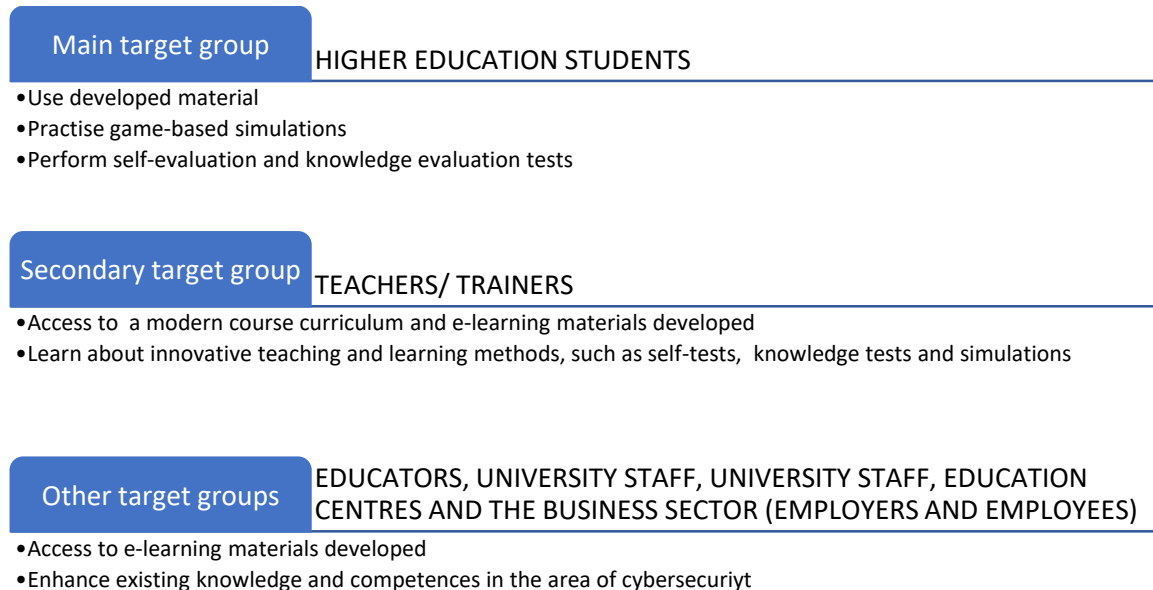


Figure 1 Target groups of the project

Training duration. The recommended period of the training is 4-6 weeks. The entire curriculum is 30 hours; it is equivalent to 1 ECTS. It is suggested that the same number of hours per module be considered for self-study and assessment. It is recommended that participants spend 2-3 hours per week during the course (reading training material, solving tests and scenarios).

The estimated training time may vary depending on the training. The topics and exercises/scenarios provided are divided into one-day sessions. The amount of time allocated is flexible; therefore, an exact timetable for each day is not provided.

The trainer should review the material in advance and plan the time to suit the specific training needs.

Course structure. The Course Curriculum is structured in four parts:

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

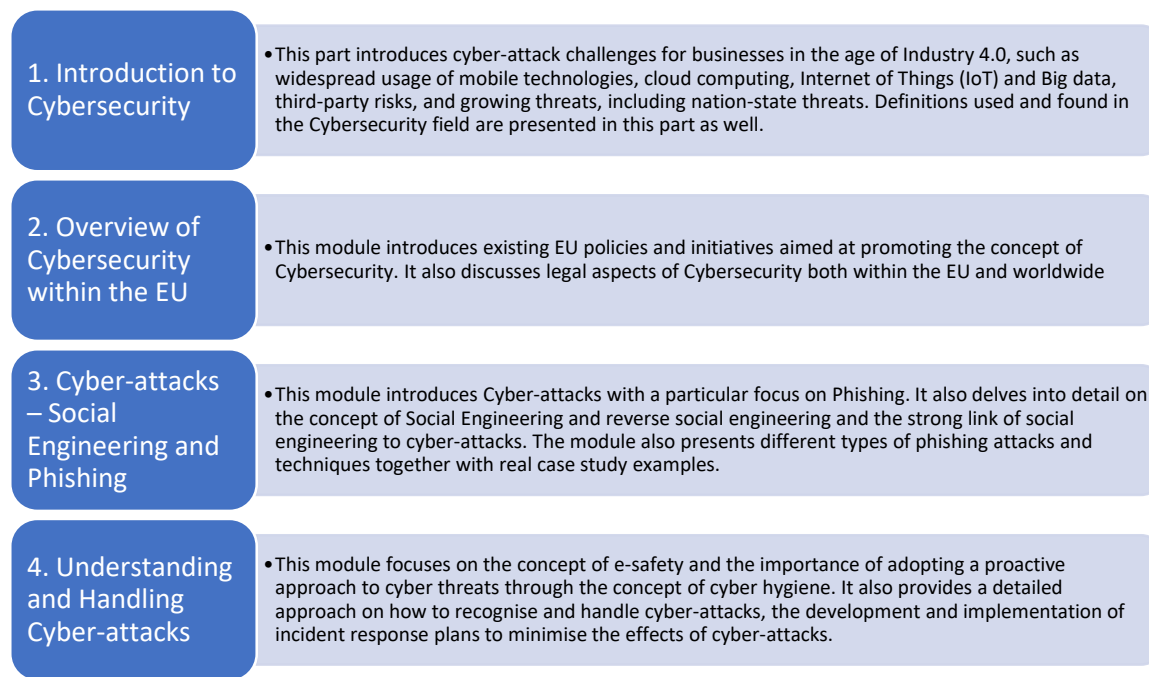


Figure 2 Structure of the course

The detailed curriculum can be found on the project webpage www.cyberphish.eu

Short version: https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A1_Short-version-of-curricula-for-dissemination_EN.pdf

Full version: https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2_Extended-version-of-curricula_EN.pdf

COMMON PROCEDURES FOR TRAINING

This part guides organising training. Here we also include good practice recommendations used during CyberPhish pilot training, including a questionnaire before training, requirements for participant's registration, the learning process and conditions for a knowledge test.

Call for training

Suppose the training is organised as a separate course which is not included in the curriculum of the higher education institution. In that case, it is recommended to publish an announcement inviting participants to the pilot training on the website and/or on social networks or to send a personal invitation to potential participants by email. This invitation informs a potential participant on the primary goal of training, course duration, developed or obtained competences in recognising phishing attacks and certification after completion of the course. It also could contain the link to the registration form.

An example of an invitation is given in Annex 1. Files in ppt and pdf formats are available in the <https://wiki.cyberphish.eu/>.

Introductory meeting

At the beginning of the course, during the first meeting, it is important to build trust between the trainer and the participants, to motivate them, and to let them get to know each other. Introduce the form of the consultation (live/ distance) and the frequency, for example, weekly, three times per course (at the beginning, end, and middle). It is recommended to mention challenges then may occur during registration to the platform (e.g., the confirmation email going to spam folder).

During the meeting, participants are explained how to use the e-learning environment, are allowed to try it out and are invited to share any problems they may have, so there are no uncertainties later on when the course starts. The meeting also includes an introduction to the CyberPhish Course.

Questionnaire before training

To assess the impact of the training on participants' knowledge progress, it is recommended to use a questionnaire before training starts. During the pilot training, partners used questionnaires which consisted of 20 questions. The questionnaire was developed in English and localized in the languages of the partners' countries: Estonian, Greek, Latvian and Lithuanian.

The questions were selected from the self-assessment questions (20 out of 60). All participants were given the same questions, but in a different order. This questionnaire does not impact on the results of the participant, but it allows measuring the change in participant's knowledge.

The questionnaire takes between 20 and 25 minutes to complete. Before completing the questionnaire, participants must provide their email address. It is recommended to use the same email address when registering for the course learning environment (www.cyberphish.vukhf.lt). Participants should be informed that they have to use a valid email address. The same email address has to be used in the learning environment, as on the participant's registration form.

It should be noted that it is not compulsory to conduct a pre-training questionnaire. It is only a recommendation, but this practice could be used if you are interested evaluating the impact of training course on participants.

Online training

After a short introductory phase, the online training starts and lasts about one month (4-6 weeks). During the training process the participants are involved in various learning activities using a variety of training methods and forms which cover, but not limited to studying e-learning material, reading additional material, watching videos related to the topics, doing self-evaluation tests and knowledge evaluation tests, and solving simulations. During this time, participants learn about cybersecurity, understand cyber-attacks and social engineering, learn how to recognise the main signs of phishing, understand the handling of cyberattacks, learn to minimize damages through incident response. Successful participation in the training depends on the participants' ability to plan their own time and activities, and collaboration with trainers and other team members.

The training should result in the successful completion of a knowledge evaluation test (score of at least 75%) and the award of an automatically generated certificate. At the end of the training, participants gain new knowledge and skills that they can use in their everyday life (such as searching the internet, personal communication on social networks, talking on the phone with strangers, studying, in their workplaces, ect.). In addition, they also boost their confidence.

Structure of e-learning environment

Cyberphish.vuknf.lt learning platform provides open access to learning materials. The material can be studied freely by all persons who wish to do so. No registration is required. However, to be able to solve simulations that teach how to recognise phishing attacks, do self-tests, knowledge assessment test and to obtain a certificate, it is necessary to be a registered user.

Learning material. By clicking on the *Learning material* button in the menu bar, the user can see the course modules on the left of the screen. There are four modules: Introduction to Cybersecurity; Overview of Cybersecurity within the EU; Cyber-attacks – Social Engineering and Phishing; Understanding and Handling Cyber-attacks. Each module consists of several topics. Once a case is selected, the learning material is displayed in the central part of the screen. User can download the material can be downloaded to the user's computer by clicking on the *Download slides* link.

Self-evaluation tests. Registered users have more options. They have the opportunity to take self-evaluation tests for learning purposes. The *Self Evaluation test* button appears when a student has learned the module material. Therefore, the student must click the button *Completed* when he or she is familiar with each topic in the module. When all the topics in the module are marked as *Completed*, which means that the material in that module has been learned, then the opportunity to take the self-evaluation test is available by clicking on the *Self Evaluation test* button. During the test, the student is presented with five random questions from that module.

After the test, the system displays test results, showing the answers chosen by the student, the correct and incorrect answers, the time taken to solve the test, and the points scored. The student can retake the test by clicking on the *Do*

it again button. When retaking the test, 5 random questions are presented. The student can take the self-evaluation test an unlimited number of times.

Simulations. Registered users can solve simulations. These simulations are mock-up of an actual situations. On the left side of the screen, there is a *Simulations* button above the module topics. The student at any time can solve these. The simulations are grouped into 7 groups: Unity, Liking, Consensus, Consistency, Authority, Scarcity and Reciprocation. When a simulation is selected, a description of the situation is given. Simulations can operate in two modes: for learning purposes and knowledge testing purposes. In the first mode, the student sees the scores collected and the overall conclusion at the end of the simulation. In a simulation for knowledge testing, the student considers the choices made during the simulation at the end and receives feedback with comments. The mentor should decide how many simulations the participant has to solve. For example, during the Pilot each participant had to solve a minimum of 20 simulations of their or his choice.

Knowledge evaluation test. Registered users can take the Knowledge Test and receive a Certificate. The *Knowledge Test* button appears on the left side of the screen above the course modules when the student has learned all the material and marked all the topics as completed. The test is considered to be passed if a score of at least 75% is achieved. Participants who pass this final test will receive a certificate. If the participant does not pass the test, he or she can repeat the topics and, after spending some more time learning, he or she can retake the final Knowledge test. The knowledge test can be taken three times.

Ratings. The system calculates ratings to make the learning process more attractive to students. The course participant can see his or her rating and the points he or she collected in the overall rating table. The ratings are based on self-evaluating tests and simulations. The ratings can be accessed via the menu item *Ratings* at the top of the screen. The student's simulation rating is calculated by summing the best results of all simulations solved. Correspondingly, the student's self-evaluation test rating is calculated by aggregating the top scores of all self-tests taken.

The students can also see their learning progress. It is displayed above the course modules on the screen's left and via the user menu at the top of the screen. Through the user menu, the student can change the username, and password, see the badges collected, the history of the self-tests and the history of the simulations.

Certificates. Certificates (in PDF format) are automatically generated for all participants who have completed the course and passed the Knowledge-Evaluation Test at least 75%. An example of certificate is given in Annex No. 2.

Certificates will be awarded to all participants upon completion of the course. Completing the CyberPhish course does not award academic credit.

The availability

The developed e-course is available in four languages: English, Estonian, Greek, Latvian and Lithuanian. It is hosted on <https://cyberphish.vuknf.lt/>. A picture of the main screen of the learning platform is given below.



Figure 3 The main screen of the learning platform

Good practice recommendations from Pilot training. It is recommended to develop rules and instructions for students. Questionnaires at the beginning and the end of the course are optional. Other tools can be used as in regular training.

Instructions for the students

In this part, we provide recommended steps by organising training:

Step 1. Pre-training questionnaire. Before the training, complete the questionnaire. Provide a valid email address which will also be used in the e-learning system on completing this questionnaire.

Step 2. Sign in to the e- learning environment. Sign in to the e- learning environment on <https://cyberphish.vuknf.lt/login> with the same email address used in the questionnaire.

Note: If the student has not received the confirmation email from the system, it is necessary to check the spam folder. The confirmation email may end up in the spam/junk folder.

Step 3. Log in to the e- learning environment.

Login on <https://cyberphish.vuknf.lt> with personal credentials.

Step 4. Studying of Learning material.

After logging in, study all the training material, i.e. four topics and subtopics (see below). Mark as *completed* after going through each topic.

Topics and subtopics:

1. Introduction to Cybersecurity;
 - 1.1. Background – Challenges of the 4th Industrial Revolution;
 - 1.2. History of Cybersecurity;
 - 1.3. Definitions of Cybersecurity
2. Overview of Cybersecurity within the EU;
 - 2.1. Fostering Cybersecurity within the European Union;
 - 2.2. Legal Aspects of Cybersecurity;
 - 2.3. Overview of the tendencies of the cybersecurity landscape;
3. Cyber-attacks – Social Engineering and Phishing;
 - 3.1. Introduction to Cyber Attacks;
 - 3.2. Social Engineering Modules and Manipulation;
 - 3.3. Different Types of Phishing Attacks and Techniques;
 - 3.4. Case Studies;
4. Understanding and Handling Cyber-attacks.
 - 4.1. Basic Knowledge on e-safety;
 - 4.2. Proactive actions;
 - 4.3. Recognising Phishing Attacks;
 - 4.4. Handling Cyber Attacks;
 - 4.5. Minimising Damage through Incident Response,

Step 5. Complete Four Self-Evaluation Tests. After learning each topic, complete the Self-Evaluation Test.

Step 6. Run/Resolve/Perform Simulations. During the learning, perform simulations as a part of the study process.

Step 7. Complete Knowledge-Evaluation test. Finally, pass the final test with a score of at least 75%.

Step 8. After passing the final test, fill in a **Post-Course Questionnaire for participants** about the Pilot training.

Note: this tool was used during the pilot training, but other tools can be used as in regular training.

Final meeting

The final meeting has several purposes: firstly, it allows participants to fill in a post-training questionnaire, secondly, it will enable participants to express their views on the course. Finally, the process of knowledge assessment tests, the difficulties and challenges of answering the questions and other issues could be discussed.

Post-Course Questionnaires

In a Pilot, participants were asked to fill in a **Post-Course Questionnaire for participants** after passing the final test. The questionnaire consists of points asking to provide general information such as email, gender, occupation and questions about the evaluation of participant's knowledge in particular cybersecurity subjects after finishing CyberPhish training course, participant's experience using simulations. Furthermore, questions about the course objectives, eligibility of online format approach, course content, time duration, training and support, learning platform usability are also asked. The example of the questionnaire is given in Annex No. 3.

Trainers and mentors were asked to fill in a **Post-Course Questionnaire for trainers** after the Pilot as well. The questionnaire consists of points asking to provide general information such as email, name, country, as well as questions about the structure and content of the course, time duration, relevancy of topics to target audience, completeness of course topics, the extent to which the course has achieved its objective introducing cybersecurity and phishing to students. The example of the questionnaire is given in Annex No. 4.

DESCRIPTIONS OF HOW TO WORK WITH E-PLATFORM

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.

The user manual is provided in the document **User_Manual_for_training-Participants.pdf** on the <https://wiki.cyberphish.eu/>. This document describes how to use the learning platform.

Teachers environment

In the teacher's environment, you can monitor the participants registered in the learning system, their learning progress in percentage terms, the history of self-tests taken, the history of simulations, the grades of the knowledge test, and the date and time of the last login.

Login address to the Teacher Environment: <https://cyberphish.vuknf.lt/admin-panel>. Login window is given below:

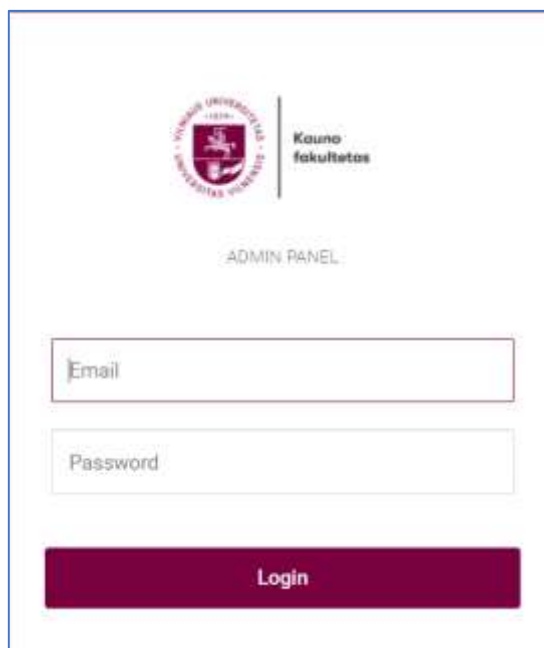


Figure 4 Login window to the Teacher Environment

Once the login details have been entered, the system provides the teacher with a list of participants. The teacher can monitor the participants' learning progress by language (English, Lithuanian, Estonian, Greek and Latvian). The main screen of the teacher's environment is given below:

| Username | Email | Course Progress | Self Evaluation | Simulations | Knowledge results | Last Login |
|-----------------|-----------------------|-----------------|-------------------------|------------------------------|-------------------|---------------------|
| User [redacted] | [redacted]@gmail.com | 10% | Self Evaluation History | Simulations History (2) / 1) | | 2022-07-16 11:25:38 |
| User [redacted] | [redacted]@gmail.com | 0% | Self Evaluation History | Simulations History (2) / 0) | | 2022-07-14 15:18:23 |
| User [redacted] | [redacted]@stud.vu.it | 0% | Self Evaluation History | Simulations History (2) / 0) | | |
| User [redacted] | [redacted]@gmail.com | 0% | Self Evaluation History | Simulations History (2) / 0) | | 2022-07-12 08:08:38 |

Figure 5 Main screen of the teacher's environment

Self-evaluation tests history

This details are seen by clicking on participant's Self-Evaluation History:

| Category | Correct answers | Started | Ended | Points |
|-------------------------------|-----------------|---------------------|---------------------|--------|
| Introduction to Cybersecurity | 4/5 | 2022-07-17 09:00:16 | 2022-07-17 09:01:58 | 431 |
| Introduction to Cybersecurity | 3/5 | 2022-07-17 08:49:56 | 2022-07-17 08:50:45 | 98 |
| Introduction to Cybersecurity | 0/5 | 2022-05-03 12:40:15 | | 0 |
| Introduction to Cybersecurity | 0/5 | 2022-05-12 10:02:25 | | 0 |
| Introduction to Cybersecurity | 0/5 | 2022-05-13 10:44:42 | | 0 |
| Cybersecurity within the EU | 0/5 | 2022-07-17 09:06:23 | | 0 |

Figure 6 Self-evaluation history of participant

Simulations history

These details are seen by clicking on participant's simulations history:

| ID | Description | Started | Ended | Points |
|----|---|---------------------|---------------------|--------|
| 38 | As Bitcoin and other cryptocurrencies surged in price and popularity, hackers and cybercriminals became more interested in stealing it. You are aware of the current profitability of bitcoin and you have received an email concerning bitcoin: FIRST PAYOUT IS READY FOR YOUR CONFIRMATION Dear customer, Thank you for participating in our bitcoin program, we want to inform you that your bitcoin bonus is now available and ready to be withdrawn. | 2022-06-09 18:14:10 | 2022-06-09 18:16:07 | 600 |
| 2 | You're receive an email about winning money. | 2022-06-09 18:16:27 | 2022-06-09 18:17:15 | 500 |
| 4 | You are an accountant who has worked for company "Future Solutions" for 35 years. You communicate with your boss, John Smith, on a daily basis by email. This morning you received an email from your manager asking you to read a document and let him know if you agree with a new company policy. | 2022-06-09 18:17:59 | 2022-06-09 18:18:36 | 500 |
| 6 | You are a company accountant and receive an email from your partner company requesting to transfer funds. In the email there is an ask to update bank account details, as your partner has switched their banking provider. It sounds like a legit request as you get them from time to time. | 2022-06-09 18:20:35 | 2022-06-09 18:20:50 | 200 |
| 8 | You are a company accountant and receive an email from your partner company requesting to transfer funds. In the email there is an ask to update bank account details, as your partner has switched their banking provider. It sounds like a legit request as you get them from time to time. | 2022-06-09 | 2022-06-09 | 100 |

Figure 7 Participant's simulations history



WORKING WITH INNOVATIVE METHODS (I.E. SIMULATION METHODS, LECTURES, SEMINARS, PRACTICAL TRAININGS, INTERNET TOOLS USAGE ETC.)

Simulation imitates actual phishing attacks by presenting the process to the user in a playful form.

The main aim of the simulation is to help people to improve critical thinking related to cybersecurity and phishing by recognising cases of phishing, spam, cyberbullying etc. Based on [IO1](#) recommendations were developed for simulations —focusing on adapting real life case studies for the learning process.

The simulation includes a description of the situation, the purpose, the characters, the type of attack and several (3-4) answer options for user behaviour. The simulations were designed to assess the possible/probable conduct of the user, his or her potential considerations/concerns and decisions in such a situation. The simulations presented consist of three levels of depth. Once one of the problem/situation options has been selected, further possible options for the case to be solved are affected and presented.

Simulation for learning purposes and for knowledge testing purposes are implemented. When solving a simulation for learning purposes, the student sees the scores collected and the overall conclusion at the end of the simulation. Solving simulation for Knowledge testing purpose, the student sees the choices made during the simulation and receives feedback with comments at the end of the simulation. If the simulation was solved incorrectly, the user is recommended to solve the simulation again.

CONCLUSIONS AND RECOMMENDATIONS

This document is developed for all trainers and mentors who provide advice and training to students. Project consortium hopes that they will find useful guidance on how to use the system and how to provide training to people who want to learn about cyber-attacks, in particular, phishing and social engineering, as well as who want to learn how to recognise the main signs of such threats. Potential users are required to have basic digital literacy skills. There are no other prerequisites for user's knowledge or skills.

Students, and employees lack knowledge about phishing, social engineering, cyber-attacks and the security of their data, according to a study carried out by project partners in 2020 in Estonia, Cyprus, Latvia, Lithuania and Malta (see https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A1-Report_Recognising-Phishing-and-Skills-Gaps_EN.pdf).

This leads not only to loss of personal data and personal finances in case of phishing or cyber-attack, but also to loss of sensitive information and financial resources of companies/organisations.

Based on a study (see https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A2-Report_Analysis-of-existing-Cybersecurity-training-programmes_EN.pdf) carried out in the partner countries on higher education curricula related to cybersecurity, as well as on the cybersecurity training programmes provided by private companies, a curriculum has been developed, covering four modules:

- Introduction to Cybersecurity;
- Overview of Cybersecurity within the EU;
- Cyber-attacks – Social Engineering and Phishing;
- Understanding and Handling Cyber-attacks

For more information on how to prepare trainers and mentors for the training, see the full CyberPhish course curriculum (see https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2_Extended-version-of-curricula_EN.pdf)

The CyberPhish training course was well received by the participants in the pilot training. They acknowledged its usefulness in the daily IT-related activities of both ordinary users and company employees. More information will be provided in the report IO6 A2: Guidelines for course implementation.

The online learning course integrates the training material in PDF format - in a concise and clear way, without overwhelming the trainees with a lot of reading. For those who want to learn more about a specific topic, links to external sources are provided at the end of each PDF document.

Self-evaluation tests and Simulations are used to help participants better assimilate the training material. The Simulations provide feedback, which helps either to review the training material or to learn new things. In addition, simulations can be used in two modes during the course: for learning and knowledge testing.

The course can be intended for students as part of a course, as supplementary material, or as a separate module/course.



REFERENCES

1. IO1 A1: Recognising Phishing and Skills Gaps report
https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A1-Report_Recognising-Phishing-and-Skills-Gaps_EN.pdf
2. IO1 A2: Analysis of existing Cybersecurity training programmes report.
https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A2-Report_Analysis-of-existing-Cybersecurity-training-programmes_EN.pdf
3. IO2 A1: Short version of curricula for dissemination
https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A1_Short-version-of-curricula-for-dissemination_EN.pdf
4. IO2 A2: Extended version of curricula for training material development and for trainings
https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2_Extended-version-of-curricula_EN.pdf
5. User_Manual_for_training-Participants.pdf <https://wiki.cyberphish.eu/>

Annexes

Annex 1. Example of online invitation for to CyberPhish course

**We kindly invite you to participate in the
online course about phishing!**

Registration to online training: <link>

 Duration of pilot training **4-6 week**

 You will learn about **phishing attacks** through an online training material and a scenarios in which you will have to recognise whether or not it is a phishing case and what actions you would take in such a situation.

 The scenarios tool will help you **better understand fraud** and **gain knowledge interactively**.

 All course participants completed the course will be **awarded certificates**.
Participants completed course with highest scores will be **awarded prizes**.

 **Course participants will develop competences that will help them to highlight threats and take appropriate preventive measures.**

 More information about the **CyberPhish project**:
<https://cyberphish.eu/>

Trainings are organized in the framework of the CyberPhish (Safeguarding against Phishing in the age of 4th Industrial Revolution) project which is funded under the Erasmus+ programme.

 **CyberPhish**
Safeguarding your digital future

 Funded by the
Erasmus+ Programme
of the European Union



Example of printed invitation form to CyberPhish course

We kindly invite you to participate in the online course about phishing!

Registration to online course:

Name and Surname _____

Name of education institution _____

Email _____



Duration of pilot training **4-6 week**.



You will learn about **phishing attacks** through an online training material and a scenarios in which you will have to recognise whether or not it is a phishing case and what actions you would take in such a situation.



The scenarios tool will help you **better understand fraud** and **gain knowledge interactively**.



All course participants completed the course will be **awarded certificates**.

Participants completed course with highest scores will be **awarded prizes**.



Course participants will develop competences that will help them to highlight threats and take appropriate preventive measures.

Trainings are organized in the framework of the CyberPhish (Safeguarding against Phishing in the age of 4th Industrial Revolution) project which is funded under the Erasmus+ programme.

All personal data contained in this document is collected during the implementation of the Erasmus + Program (2014-2020), according to the European Commission's regulations. These will be stored and processed by Program Beneficiary Organizations, NA, EC in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of these data and repealing Directive 95/46 / EC (General Data Protection Directive - GDPR). The beneficiary organizations of the Program, EC, NA will store and process these data according to Regulation (EC) no. No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. During the event, photographs and / or films will be taken for purposes of promoting and disseminating the results of Erasmus + funded projects. The materials will not affect your personal or institutional image. By registering to this event you consent to being filmed and / or photographed for the aforementioned reasons.



Annex 2. Example of a CyberPhish course completion certificate

CERTIFICATE
OF COMPLETION ONLINE COURSE

Name Surname

has successfully completed the online training course

Safeguarding against Phishing in the age of 4th Industrial Revolution

This certificate was awarded on 12 May, 2022

 CyberPhish

Project funding source: Erasmus+ KA2 Strategic Partnerships.
CyberPhish Project No 2020-1-LT01-KA203-078070,
<https://cyberphish.eu>

Funded by the
Erasmus+ Programme
of the European Union 



Annex 3. Example of Post-course questionnaire for CyberPhish course participants



Post-Course Questionnaire for participants

This survey is part of an EU funded CyberPhish project to design and develop e-learning materials, blended learning environment, knowledge and skills self-evaluation and knowledge evaluation system simulations for students and other users in order to prevent from phishing attacks, raise competencies in this area for identification and prevention of threats.

This survey will gather information from course participants who have completed the CyberPhish course. The data will only be used for the purpose of the project.

The survey should take approximately 10-15 minutes to complete.

Thank you for your cooperation and your time.m



[redacted]@gmail.com (nebendrinama)

Perjungti paskyrą



*Privaloma



Gender *

- ☐ Male
- ☐ Female
- ☐ Other

Occupation *

- ☐ Student
- ☐ Employee
- ☐ Self-employed
- ☐ Business owners
- ☐ Other



How would you evaluate your knowledge on these cybersecurity subjects after finishing the CyberPhish course *

| | I have gained a lot of new knowledge about phishing | I have improved my knowledge about phishing | I haven't learnt anything new |
|---|---|---|----------------------------------|
| Legal Aspects of Cybersecurity | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| The tendencies of Cybersecurity landscape | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Social engineering | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Psychological aspects of social engineering | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Types of Phishing Attacks and Techniques | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Recognising Phishing Attacks | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Proactive actions of cyber incidents | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Handling Cyber- attacks | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |



How would you evaluate your knowledge on these cybersecurity subjects after finishing the CyberPhish course *

| | Satisfied | Neutral | Dissatisfied | I have no opinion |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| Introduction to Cybersecurity | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Overview of Cybersecurity within the EU | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Cyber-attacks – Social Engineering and Phishing | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Understanding and Handling Cyber-attacks | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Your experience using simulations *

| | Strongly helped | Helped | Not helped | I have no opinion |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| Did the simulations help to improve your skills recognising phishing? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |



Please rate your experience of the following elements of the CyberPhish course? *

| | Strongly agree | Agree | Disagree | Strongly disagree |
|--|-----------------------|-----------------------|-----------------------|-----------------------|
| I had a clear understanding of the course objectives | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I found the online approach to learning was suitable for the course | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I found the course content covered the course objectives | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I found the amount of time given to complete the course to be ample | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I found the training and support throughout the course to be appropriate | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |



I would
recommend this
course to other
people

☐☐☐☐

The online
learning platform
was easy to use

☐☐☐☐

What are the main benefits you gained from completing the CyberPhish course?
(Please provide one or two sentences)

Jūsų atsakymas

Was there anything missing from the course or anything that could have been
improved? (Please provide one or two sentences)

Jūsų atsakymas

Thank you for your participation in this survey and for completing the CyberPhish course!

Pateikti



Puslapis 1 iš 1

Valyti formą

Annex 4. Example of Post-course questionnaire for CyberPhish course trainers, consultants and mentors



Funded by the
Erasmus+ Programme
of the European Union



Post-Course Questionnaire for trainers/ consultants/ mentors

This survey is part of an EU funded project to design and develop e-learning materials, blended learning environment, knowledge and skills self-evaluation and knowledge evaluation system simulations for students and other users in order to prevent from phishing attacks, raise competencies in this area for identification and prevention of threats.

This survey will gather information from CyberPhish course teachers/consultants/mentors. This survey will help to evaluate the project's pilot trainings.

The survey should take approximately 10-15 minutes to complete.

Thank you for your cooperation and your time.



@gmail.com (nebendrinama)

Perjungti paskyrą



*Privaloma



Name *

Jūsų atsakymas

Country *

- ☐ Lithuania
- ☐ Latvia
- ☐ Estonia
- ☐ Malta
- ☐ Cyprus



Please indicate how strongly you agree or disagree with the following statements *

| | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree |
|--|-----------------------|-----------------------|----------------------------------|-----------------------|-----------------------|
| The structure and content of the course motivated participants to complete it. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| The time provided for participants to complete the pilot course was sufficient. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Areas of topics covered by the course were appropriate for the target audience. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| The appropriate amount of detail was provided for the topics covered by the programme. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |



What other additional support or resources could have helped to organise the course

Jūsų atsakymas

Please indicate how much you agree or disagree with the following statement *

Fully achieved

Achieved to a
high extent

Achieved to a
low extent

Not achieved

To what extent
has CyberPhish
achieved its goal
of introducing
cybersecurity
and phishing to
students



Other comments, suggestions

Jūsų atsakymas

Thank you for your participation in this survey and for completing the CyberPhish course!