Erasmus+ KA2 - KA220-HED - Cooperation partnerships in higher education
2021-1-TR01-KA220-HED-000031993

Cyber in Practice

“Cybersecurity in practice for non IT oriented HE courses”

Project

TESTING METHODOLOGY

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". “This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

Main Contents

Introduction 3

The training environment model 4

The Training contents-The Nuggets 4

The Cyber in Practice e- platform in Moodle 6

Testing Methodology 7

The structure of the testing – target groups, activities and duration 7

The Target Groups 8

The Pilot Testings and the duration 8

The Feedback Questionnaire 10

Annex_ Feedback Questionnaire 13

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". “This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

Introduction

“The Testing Methodology (R23/A4) for integration of the nuggets into non IT disciplines” aims at supporting trainers and educators in making use of the Cyber IN Practice outputs and in implementing future training courses or units of cybersecurity knowledge into their courses based on the materials created. The present training methodology wants to define tools and methods to implement the CyberinPractice trainings in order to guide trainers, adult educators, teachers and stakeholders in the implementation of the training material in their organization to learners interested in cybersecurity management issues. In addition the document describes the methodology to be used by the partner countries to carry out the pilot testing foreseen within the project(R3-A4). This Pilot testing will be carried in each partner country for testing the Cyber in Practice approach for incorporation of IT knowledge into the learning content of non IT disciplines. In this sense, the following Training and Testing Methodology describes the target groups, the processes, the activities, the timing and the tools to be followed during the testings of the Cyber in Practice training material and platform that will be evaluated by trainers, educators and students from non-IT disciplines involved in the testing phase.

The testing methodology evaluates the following project outputs of Result 2 :

1. The training contents in the form of the micro learning nuggets;
2. The Cyber in Practice learning platform in Moodle with the available online learning material.

The final feedback questionnaire which will be used for the evaluation of the training according to the testing methodology is presented in this document.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". “This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

The training environment model

The training model is based on two main elements:

1. The Cyber In Practice training contents- **micro e-learning nuggets**

2. The use of interactive ICT tools/Moodle platform for training.

The contents will be provided in the form of online learning nuggets available on the Cyber in Practice Moodle Platform.

The Training contents-The Nuggets

The Online micro learning nuggets are part of the Result 2 "*Development of Guide with learning nuggets"* of the Cyber In Practice project. The main aim of R2 is to provide non IT teachers, teacher educators, education practitioners and students with "nugget" knowledge necessary to protect themselves and their students online, as well as to create awareness for other stakeholders in digital learning. Each learning nugget is developed as follows:

1. **Introduction/use-case/infographic** presenting the learning objectives for developing specific competences

2. **Theory:** a short video or interactive presentation (3-5 minutes) as the nutshell of information, only the most important things

3. **Assessment quiz game**: A stand-alone resource to support performance ('just-in-time) evaluation.

The project partners have identified in R2 different areas of interests for the learning nuggets that became the main topics of the developed training material. The following table describes the areas, the nugget title, partner responsibility and number of the foreseen nuggets to be developed.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". "This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

Areas	Nugget Titles	Responsibility	Number of Nuggets
Social Engineering	Recommendations on the use of emails	EDUVIBES	10
	Phishing examples and analysis of email phishing /pharming		
	Skimming		
	Vishing		
	Smishing		
Content related risks	Recognition of Fake news on digital media	ULSIT	10
Technology-focused threats	Hacked applications, update threats	Training2000 &SUPSI	10
	Hacked websites, how to check certificates and control Ips		
Risk of exposing information (also under technology if we considered Authentication/ authorization)	Steps for planning virtual thesis defense meeting (the main target group master and PhD students)	MSKU &MU	10
Security incidents	Institutional attacks	Training2000 &SUPSI	10
	Attacks against individuals		
Privacy violations	Institutional & Individual violations	MSKU &MU	10
Harassment related threats	Cyber- bullying, cyber-stalking and other forms of unwanted contact	ULSIT	5

The areas identified as the most relevant aspects of cybersecurity to be further analyzed are ***"Social Engineering", Content related risks, Technology-focused threats, Risk of exposing information, Security incidents, Privacy violations, Harassment* related threats** . These thematic areas can refer to more than one topic as listed in the table above. The partners have defined learning outcomes, in terms of knowledge, skills and abilities within each nugget and have developed interactive training material (H5P model) to allow users to evolve and enhance their personal and professional competences in the specific topics.

The Cyber in Practice e- platform in Moodle

The micro learning nuggets of Cyber in Practice project have been developed with the h5p tool. It provides flexibility, is equipped with all necessary features and offers the possibility to create open education resources for a wider audience. More specifically, the Cyber in Practice Moodle platform houses 65 learning nuggets in 7 macro areas in the form of interactive material, videos, ppt files, infographic, tests and quizzes. The Cyber in Practice Moodle platform will be subject to the pilot testings for educators, teachers, academics, trainers and learners from non IT faculties.

Trainers, adult educators and teachers can adopt the provided material in developing their own training course in cyber security vs. cyber attacks and/or use it as a reference for the implementation of other educational material. As well learners can improve their own competences in the specific topics. During the testing with the learners, key nuggets will be chosen for testing the main tools, concepts and materials as covered in R1/A3.

The Training Nuggets and the Moodle platform as described and shown in the 'Training methodology' will be both subjected to pilot testings.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". "This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

Testing Methodology

The main results subject to the testing are the learning **Nuggets** and with their interactive training contents and **the Moodle platform** which were developed within the scope of the project.

The testing phase involves different actors and target groups from all partner countries and includes assessment activities (online questionnaires) to be completed by adult educators, trainers, adult learners-students from non-IT faculties and disciplines.

The aim of the testing phase is to evaluate the suitability and appropriateness of the materials, namely the micro-learning nuggets and the platform in order to improve and adapt them to the needs of the target groups.

The structure of the testing – target groups, activities and duration

In the testing phase, the outputs mentioned above and developed in the frame of the project will be evaluated by the participants (trainers, teachers and students of non IT faculties or with non IT background of studies). A final feedback questionnaire will be provided to the participants at the end of the pilot training.

The Pilot testing will be carried out in each partner country for testing the Cyber IN Practice approach for incorporation of IT knowledge into the learning content of non IT disciplines.

The partners will conduct at least two sessions of the testing for each of the disciplines they have selected to work on among the 7 macro areas developed within the project.

The aim of the pilot testing consists in the evaluation of the nuggets and the Moodle platform with its open educational resources carried out by trainers, teachers, educators and students from non IT disciplines, who will use the created material in the future. The pilot testing will start in Month 18 (August 2023) and will end in Month 22 (December 2023). The team will conduct pilot testing with trainers and learners in those months, by creating real conditions for teaching non-IT discipline, in which the selected nuggets of knowledge on cybersecurity and/or risk management are embedded.

During the pilot training, **participants should be able to evaluate the online platform and the training nuggets.** The trainees will be asked to identify the benefits and the critical points of all project outputs in relation to their needs to develop appropriate competencies linked to cybersecurity. They will provide suggestions to be incorporated for further improving the learning

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". "This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

material. The pilot testing will thus lead to the optimization and finalization of all the training materials produced by the partner countries.
The pilot training will focus mainly on trainers, teachers working in non IT faculties in order to evaluate the usability of the material for future implementations. As well, students of non IT disciplines will be active participants of the testing phase.

Each session of the pilot testing will be adapted by the partner according to the target, the institution and the respective discipline.

In total, **180 trainees** will take part in the testing phases of the project's outputs, 30 participants in each partner country.

The Target Groups

The target groups are the potential users of the outputs subject to testing. The target group includes trainers, teachers and students from non IT disciplines. At least 30 participants from each partner country will take part in the pilot training for a total of 180 trainees.

The Pilot Testings and the duration

The pilot sessions will be carried out in a period of 4 months M18-M22 (from August to December 2023), with each partner institution deciding how to arrange the sessions in this period and how many sessions will be held per selected non-IT disciplines by the countries. The partners adopted the rule of conducting **at least two sessions for each of the modules they have selected to work on among the following ones:**

1. *Social Engineering*
2. *Content related risks*
3. *Technology-focused threats*
4. *Risk of exposing information (also under technology if we considered Authentication/ authorization)*
5. *Security incidents*
6. *Privacy violations*
7. *Harassment related threats*

Cyber IN Practice team plans to involve at least 180 trainees (non IT students) in the pilot sessions carried out by all partners. The testing phase is foreseen to allow participants to acquire knowledge regarding the domain of cyber security, cyber attacks, technology based threats, Security incidents, Privacy violations.

The first part of the pilot training is focused on the presentation of the **online training materials in the form of micro learning nuggets,** together with **the Cyber in Practice Moodle online platform**. Trainers, teachers and students will then test and evaluate the appropriateness of the material provided in covering the agreed learning outcomes and training goals and the effectiveness of the tools. Trainees will be then invited to access the interactive online Moodle platform and **test it autonomously being mentored by trainers**. The trainers will provide them the link to access the online platform and training materials and encourage them to test **different materials** produced. The trainer will act as a facilitator to support trainees in solving technical problems, when required. Each partner will test and evaluate the developed material in their national languages or in English.

At the end of the pilot training sessions, the participants will complete an **evaluation questionnaire**. Each person participating in the training will provide feedback by compiling the feedback questionnaire to be filled in using an online system for the automatic data collection after the pilot testing. The feedback questionnaire can be found below.

Starting from their feedback, the partners will note down the most relevant elements emerging from the testing phases (critical and positive aspects, feedback, possible due improvements, suggestions etc.) in order to implement the necessary changes. The feedback evaluation will provide ground to make changes if needed and improve the outcomes to final results.

Each partner will produce a national report with the data collected. Each national report will be combined with the others and a single international report will be prepared to indicate the improvements and changes where needed to be applied in the learning nuggets and the Moodle platform as a part of the quality process.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". "This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

The Feedback Questionnaire

The basic tool to collect the feedback for the testing processes is the questionnaire. The feedback questionnaire to be applied in each country is listed below. Each person participating in the pilot testings will fill in one individual questionnaire.

Project partners need to use online tools such as Google Form to be able to share xls data and graphics.

The participants will be asked to fill in the questionnaire honestly and carefully, thus supporting the reliability of the data collected.

A) OVERALL QUALITY

1) Please tick the best option that reflects your opinion corresponding to the statements (1 – strongly disagree; 2 – do not agree; 3 – undecided; 4 – agree; 5 – totally agree):

- The overall quality of the Cyber in Practice training materials is very good.
- The learning nuggets produced are clear and easy to understand.
- The training material is valuable for me to gain new knowledge and skills.
- I will utilize the knowledge and skills gained during the training in my life.

2) Please tick the best option that reflects your opinion corresponding to the statements (4 – very valuable, 3- valuable, 2- not very valuable, 1- not valuable at all)

  - How valuable are the training nuggets in helping you gain new knowledge and skills on cybersecurity, best behaviors to avoid cyber attacks and possible actions to be carried out to face these attacks ?
  - How valuable are the learning nuggets in helping you introduce the required competences to face cyber attacks in your daily tasks?

B) **QUALITY of the Learning Nuggets**

1. Please rate how satisfied are you with the content of the learning nuggets of Cyber in Practice Project (4 – excellent, 3-good, 2-poor, 1- very poor):

- I am satisfied with the content of the Nugget n.1 –Area of Social Engineering
.....

2. Please state **WHAT** could be **changed/improved** in terms of the content of the learning nuggets? ....

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". "This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

C) *QUALITY OF E-LEARNING PLATFORM*

1) Please tick the best option that reflects your opinion corresponding to the statements (1 – strongly disagree; 2 – do not agree; 3 – undecided; 4 – agree; 5 – totally agree):

- The interface of the Cyber in Practice Moodle platform is user-friendly.
- The digital tools in the Moodle platform are innovative
- The quantity of digital learning material is adequate

2) Please state if the Cyber in Practice Moodle platform has met your needs. What could be changed or improved in the Moodle platform?

....

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". “This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors’ view and Movetia is not responsible for any use that may be made of the information it contains”.

The national reports and the summarized international report

A national report to summarize the processes, the activities, the feedback, the improvements and the changes needed will be prepared. Each partner will take responsibility in the preparation of the national report after the pilot testing.

This section provides a framework of the content which will be used as a guidance in the preparation of the national reports. The data collected after the pilot testing will be used in the national reports and presented in the xls files and the graphics. The tested results – the learning nuggets and the Cyber in Practice Moodle platform - will be improved according to the data collected.

The framework of the national report is mentioned below:

Introduction	An introduction that describes the target group and how the pilot testings were organized will be presented.
Pilot Testing Evaluation	The survey results are presented. The XLS files, the graphics, the tables, the charts are used by the partners to present the data. The answers given by the participants in the pilot testing are compiled and summarized. The strengths and the weaknesses are determined based on the findings. A proposal for possible improvement to reduce weaknesses should be made.
Conclusions and General Evaluation	The report is finalized by making an overall assessment of the quality of the products tested and a conclusion about the results analyzed is written.

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein". "This project has received grant support from Movetia funded by the Swiss Confederation. The content reflects the authors' view and Movetia is not responsible for any use that may be made of the information it contains".

Eduvibes will combine all reports and produce 1 general report in English as an international report after the pilot testing. All partners will translate the executive summary of the report in their languages.