Cyber in Practice

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

R3/A4

FINAL REPORT ON RESULT 3

Table of Contents

1- Introduction

This document serves as a comprehensive report summarizing Result 3 of the Cyber IN Practice project. It is structured into three main sections for clarity and depth of analysis:

Implementation Guidelines Overview: The first section provides a detailed summary of the guidelines developed for the implementation of learning nuggets. This outline includes the theoretical underpinnings, the pedagogical framework, and the operational strategies recommended for effective deployment.

Methodological Framework: The second part of the report presents the methodology employed in the pilot testing phase. This includes the design, the participant selection process, the tools and techniques used for data collection, and the criteria for evaluation. The methodology section aims to ensure the reproducibility of the results and to validate the testing procedures used across different settings.

Analysis of Testing Results: The final section details the testing results as implemented across all partner countries. It highlights the strengths and weaknesses observed in the project, providing a critical analysis of the outcomes. This section not only showcases the impact and effectiveness of the learning nuggets but also discusses feedback gathered from participants. Insights into possible improvements and strategies for future enhancement of the project are thoroughly explored.

This report aims to furnish stakeholders with a deep understanding of the project's current efficacy and areas for development, ensuring informed decision-making for future iterations of the Cyber IN Practice project.

2- Implementation Guide

This activity outlines the methodological framework for implementing learning modules containing "nuggets" of cybersecurity and risk management knowledge. It's intended to support university staff, particularly in non-IT disciplines, by enhancing their ability to address cyber threats and manage risks, especially in remote teaching environments.

The idea of this guideline is to introduce practical methods, methodological tools, and instruments for design, development, and use of: learning activities, tasks, and grading methods. The methodology contains:

1. Learning nuggets in HE: practices, approaches, lacks/gaps;
2. Syllabus;
3. Teaching and learning objectives;
4. Teaching/learning strategy;
5. Evaluation of the process and its results and lessons learned;
6. Grading system/scale;
7. Thesaurus/Glossary of terms;
8. Recommendations foreseen for integration of the training material(s) into the main content of the relevant disciplines (approaches and, tools to be used)

3- Pilot-Testing Methodology

The targeted groups, comprising trainers, teachers, and students from non-IT disciplines, had included 30 participants from each partner country in the pilot training.

The pilot sessions were conducted over a period of four months from August to December 2023 (M18-M22). Each partner institution had decided on the arrangement and frequency of sessions during this period for selected non-IT disciplines. A minimum of two sessions for each module was mandated, covering topics such as;

- Social Engineering,
- Content-Related Risks,
- Technology-Focused Threats,
- Risk of Exposing Information,
- Security Incidents,
- Privacy Violations,
- Harassment-Related Threats.

The Cyber IN Practice team had aimed to engage at least 180 non-IT students in these sessions, facilitating knowledge acquisition in cyber security and related areas.

Feedback was primarily collected through questionnaires, with each participant required to fill out an individual questionnaire using tools like Google Form for data sharing. Questions addressed the overall quality and specific aspects of the training materials, including their

clarity, usefulness, and application in real-life scenarios. Participants were also asked to rate the quality of the learning nuggets and the e-learning platform, specifically focusing on user-friendliness, innovation, and adequacy of digital tools and material.

The feedback aimed to enhance the reliability of data collected, helping to assess and improve the educational content and platform based on the participants' experiences and suggestions.

4- Pilot-Testing Results Across Partner Countries

This report synthesizes the findings from the pilot testing of cybersecurity training modules conducted in Turkey, Italy, Bulgaria, Poland, and Switzerland. Each section aims to provide a detailed analysis of the participants' feedback on the overall quality of the training, the learning nuggets, the e-learning platform, and general evaluations. This feedback is crucial for continuous improvement and adaptation of the training materials to better suit the needs of learners.

3.1 Overall Quality:

Turkey: The training was highly appreciated for its comprehensive coverage and the practical utility of the learning nuggets. The e-learning platform was noted for its ease of use, which facilitated an effective learning experience.

Italy: Respondents were impressed with the clarity and accessibility of the learning materials. The training effectively bridged the gap between theoretical knowledge and practical application, which was particularly appreciated.

Bulgaria: Feedback highlighted a need for more dynamic presentation styles, as the content was perceived as too text-heavy. Despite this, the training was rated positively for its informative nature.

Poland: The quality of both the learning materials and the platform was highly rated. Participants valued the structured approach that clearly laid out the cybersecurity concepts.

Switzerland: The training materials were well-received, with emphasis on the detailed and clear presentation of content. However, some technical issues with video playback were noted, suggesting a need for better technical support.

3.2 Quality of Learning Nuggets:

Common Observations:

Across all countries, the learning nuggets were recognized for their succinct and focused delivery of content. The materials were generally found to be of high quality, providing valuable insights into cybersecurity practices.

Suggestions for Improvement:

- **Turkey and Bulgaria:** Participants suggested simplifying the language to make the content more accessible to non-specialists.
- **Italy and Switzerland:** There was a call for more practical examples and interactive elements to enhance engagement.
- **Poland:** Feedback indicated a desire for more comprehensive coverage of topics, with additional case studies and real-life applications.

3.3 E-Learning Platform Quality:

General Feedback:

The platform's user-friendly interface was universally praised. Its design and the quality of multimedia resources significantly enhanced the learning experience.

Specific Enhancements Recommended:

- **Interface Improvements:** Suggestions included more intuitive navigation and better structuring of content to facilitate learning.
- **Interactive Features:** Increasing interactivity through quizzes, simulations, and forums was seen as a way to enhance engagement and retention of information.
- **Accessibility:** Ensuring all materials are accessible to individuals with disabilities was also highlighted as a priority.

3.4 General Evaluation:

Strengths:

The modular design of the nuggets, allowing for targeted learning sessions, was a significant strength. The concise format was effective in keeping learners engaged and making complex information manageable.

Areas for Improvement:

- **Engagement:** Increasing the interactive aspects of both the nuggets and the platform was a recurring theme.
- **Content Relevance:** Tailoring the content more closely to meet the specific needs and contexts of different learner groups, particularly those from non-IT backgrounds.
- **Conclusions:** The pilot tests across the five countries have demonstrated the effectiveness of the cybersecurity training modules in enhancing learners' knowledge and skills. However, there is room for improvement in making the learning experience more interactive and engaging, and in addressing specific local needs. These insights will guide the refinement of the training modules, ensuring they remain relevant and impactful.

3.5 Recommendations for Future Improvements:

Enhance interactivity and practical application through case studies and simulations.

Improve technical support for e-learning platforms to ensure smooth operation.

Regular updates to content to keep pace with evolving cybersecurity threats.

This detailed feedback will be instrumental in the continuous improvement of the training modules, ensuring they effectively meet the educational needs of a diverse learner base.