IO7: Sustainability and replicability of the Game.

Table of content

1 Executive summary

The report highlights the need to make project outcomes available to a wider audience, particularly those who were not initially included in the project's development partnership. The assumption is that the main objectives of any project will find opportunities for enhancement and application to benefit local scenarios across different European situations.

To address this need, the report proposes the inclusion of transferability criteria in a manual that describes all targeted interventions, with the involvement of all members of the partnership. The manual will answer key questions such as the likelihood of replicating the training program elsewhere, the ability to adjust to different circumstances, and the potential for inspiring new and advanced training initiatives. Additionally, it will suggest interventions for the project partnership to undertake and outline key success factors for replication in other European countries.

The report emphasizes the importance of the CYBER4SCHOOLS network as a platform to disseminate project results and stimulate the interest of local stakeholders in duplicating the training opportunities in their countries, benefitting local education organizations.

Overall, the report recognizes the importance of sharing project outcomes to maximize their impact and benefits to local communities across Europe. The proposed manual provides a framework for transferring project outcomes, and the CYBER4SCHOOLS network offers a crucial platform for disseminating results and stimulating interest in replication.

2 Introduction

In recent years, there has been a growing awareness of the importance of sustainability and replicability in education and technology projects. Sustainability refers to the ability of a project to meet its objectives over the long term, while also minimizing negative impacts on the environment and society. Replicability, on the other hand, refers to the ability of a project to be reproduced in different contexts and settings.

The Cyber4Schools online educational game about cybersecurity was developed within the Erasmus+ project with the aim of educating students about the importance of cybersecurity in a fun and engaging way. As part of the project, sustainability and replicability were considered crucial factors in the development of the game.

Sustainability was achieved by ensuring that the game was designed to meet the needs of students and teachers over the long term. The game's content was carefully curated to ensure that it remained relevant and up-to-date, while also aligning with the needs of students and the evolving field of cybersecurity. The game's design also prioritized minimizing negative impacts on the environment and society. For example, the game was designed to be accessible to students with disabilities, and efforts were made to minimize the game's energy consumption.

Replicability was achieved by designing the game to be adaptable to different educational contexts and settings. The game's user interface was designed to be user-friendly and accessible, regardless of the user's technical proficiency or language. Additionally, the game's content was modular, allowing for easy customization and localization to fit different educational contexts and languages.

3 Toward sustainability and replicability of the game

In order to define different areas and possibilities of the sustainability and replicability following questions were identified and the answers were developed:

1) *How likely is the training program to be potentially replicated elsewhere?*

The training program can be for sure replicated elsewhere, but it is important to note that the curriculum needs to be adjusted accordingly to all countries' rules and the background of each country's rules related to education and cybersecurity for schools. For instance, in countries where cybersecurity regulations are more relaxed, the educational cybersecurity program may need to focus more on basic security measures, such as password security and phishing awareness. In contrast, in countries with more stringent cybersecurity regulations, the program may need to focus on more advanced topics, such as data encryption and network security.

Moreover, different countries have different educational systems, and thus the cybersecurity training program may need to be adapted to fit the country's specific educational context. For example, in some countries, cybersecurity education is primarily taught in computer science classes, while in others, it may be integrated into broader courses on digital citizenship or information literacy.

The success of an educational cybersecurity online game in a specific country will also depend on the local education system's willingness to incorporate such a program into the curriculum. In some countries, cybersecurity education is already a part of the curriculum, while in others, it may not be given as much priority. Therefore, it is essential to assess the needs and priorities of the local education system before introducing an educational cybersecurity program.

2) *Does this training program provide a basis for further development and adjustment to different circumstances?*

The answer to the question of whether a training programme provides a basis for further development and adjustment to different circumstances is a resounding "yes". A well-designed training programme should not only provide the learners with the necessary knowledge and skills but also give them a foundation upon which to build and adapt to changing circumstances.

One of the main goals of any training programme should be to prepare learners to face a range of situations and challenges in their work or personal lives. This means that the content of the programme must be relevant, practical and adaptable. If the programme is successful in achieving this goal, it will empower the learners to use their newly acquired skills and knowledge in various scenarios and contexts.

Moreover, a training programme can always be further developed to include new educational content that addresses different needs and target groups. This is particularly important in today's fast-paced and ever-changing world, where new technologies, ideas and trends are emerging all the time. A training programme that remains static and does not evolve with the times will quickly become outdated and irrelevant.

There are several ways in which a training programme can be further developed and adjusted to different circumstances. One way is to incorporate feedback from learners and trainers to identify areas that need improvement. This feedback can be obtained through surveys, focus groups or other means of evaluation. Once the areas for improvement are identified, the programme can be updated accordingly.

Another way to further develop a training programme is to take into account the specific needs and requirements of different target groups. For example, a programme that is designed for managers may need to be adjusted for frontline employees who have different levels of experience and responsibility. This can be done by tailoring the content and delivery methods to meet the needs of each group.

3) *What may others learn from this training program?*

The benefits of a well-designed training programme go beyond the immediate learners. Others can also learn from the programme, gaining knowledge and skills that they can apply in their own work or personal lives.

One area in which others may learn from a training programme is in the field of cybersecurity. With the increasing importance of digital technology in our lives, cybersecurity has become a critical issue. A training programme that teaches cybersecurity basics can equip individuals with the knowledge they need to protect themselves and their organizations from cyber threats. Others can learn from this programme by understanding the basic principles of cybersecurity and how to apply them in their own contexts.

Another area in which others may learn from a training programme is in the field of education. A programme that incorporates gaming solutions into school curricula can teach others how to make learning more engaging and interactive. Gaming has proven to be an effective tool in education, as it helps to motivate learners and make the learning process more enjoyable. Others can learn from this programme by understanding how to use gaming solutions to teach a wide range of subjects, from math and science to history and literature.

In addition to cybersecurity and education, there are many other areas in which others may learn from a training programme. For example, a programme that teaches leadership skills can help others to develop the ability to inspire and motivate their teams. A programme that teaches project management skills can help others to manage their time and resources more effectively. A programme that teaches communication skills can help others to build better relationships with colleagues, customers, and clients.

Furthermore, a well-designed training programme can also serve as a model for others to follow. By observing the structure and content of a successful programme, others can learn how to create their own effective training programmes. They can learn how to identify the needs of their learners, design engaging and relevant content, and evaluate the effectiveness of their programmes.

4) *Will this training programme be able to stimulate and inspire new and more advanced training initiatives?*

A well-designed training programme has the potential to stimulate and inspire new and more advanced training initiatives. By providing learners with a strong foundation of knowledge and skills, the programme can spark their interest in further learning and development. Furthermore, by identifying areas for improvement and incorporating new content, the programme can continue to evolve and inspire new initiatives.

In the case of a training programme focused on cybersecurity, there is a significant opportunity to expand the content and inspire new initiatives. Cybersecurity is a complex and rapidly evolving field, and there is always more to learn. A successful training programme that covers the basics of cybersecurity can serve as a starting point for learners to explore more advanced topics. This can inspire them to seek out additional training and certification programs, such as those offered by industry organizations or educational institutions.

In addition to expanding the scope of the programme by adding more modules and topics, there is also the possibility of tailoring the content to specific situations. For example, a cybersecurity training programme could include modules on how to secure personal devices and networks at home, as well as how to protect sensitive information in a work environment. Similarly, modules could be added that focus on cybersecurity risks and best practices during leisure activities, such as online gaming or social media use. By tailoring the content to specific situations, the programme can provide more targeted and relevant training for learners.

As the training programme continues to evolve and incorporate new content, it has the potential to inspire new initiatives in the field of cybersecurity. For example, learners who complete the programme may be

motivated to share their knowledge and skills with others, either through informal training sessions or by developing their own training materials. They may also be inspired to pursue further research and development in the field of cybersecurity, leading to new technologies and approaches for protecting against cyber threats.

5) **Which actions are to be undertaken by participants to transfer/share their training programmes with other organizations/public and private bodies?**

Sharing a training programme with other organizations and public and private bodies can be an important step in maximizing its impact and ensuring that more individuals benefit from it. However, the process of transferring and sharing a training programme can be complex and requires careful planning and execution. In order to successfully share a training programme with others, participants must undertake several key actions.

The first step in sharing a training programme is to tailor it to the needs of the target organization or audience. Different organizations and groups may have different needs, priorities, and levels of expertise. Therefore, the training programme should be adapted to suit the specific needs of the target group. This may involve modifying the content, delivery methods, or assessment criteria to ensure that it is relevant and effective for the target audience.

Once the training programme has been tailored, it can be shared with other organizations and public and private bodies in a variety of ways. Some common methods include:

- Hosting training sessions: Participants can organize training sessions for other organizations or groups. This may involve delivering the training programme in person or via video conferencing.
- Sharing materials: Participants can share training materials, such as presentations, handouts, or videos, with other organizations or groups. This can be done through email, social media, or other online platforms.
- Collaborating with other organizations: Participants can collaborate with other organizations to jointly deliver the training programme. This can help to reach a wider audience and share resources and expertise.
- Creating case studies and success stories: Participants can create case studies and success stories to showcase the impact of the training programme. These stories can be shared with other organizations and public and private bodies to demonstrate the value of the training programme.

It is important to note that the stories and case studies should be different for different target groups, as the needs and challenges of different organizations or groups may vary. By tailoring the stories to the specific needs of each target group, participants can ensure that their message resonates with the audience and is more likely to inspire action.

In the case of educational cybersecurity online games, there is a growing trend of adoption and integration into the curricula of schools and other educational institutions. Participants can leverage this trend by sharing their training programme with educational institutions and teachers. This can be done through online platforms and communities that cater to educators, as well as through professional development sessions and workshops.

*6) **What are the key success factors of a successful replication on other European countries?***

One important factor to consider is the translation of the game into the local language of the target country. While English is widely spoken in many European countries, it is important to recognize that not all children will have a strong command of the language. By providing a translated version of the game, it becomes more accessible and inclusive to a wider audience.

Another key success factor is the adaptation of the game to different cultural approaches. Cyber security threats and concerns may vary from one country to another. Therefore, it is important to tailor the game to address the specific cyber security issues that are prevalent in each target country. This requires a deep understanding of the local culture and how it perceives and deals with cyber security threats. For example, in some countries, children may be more inclined to share personal information online, while in others, they may be more concerned about identity theft or cyberbullying. By adapting the game to local contexts, it becomes more relevant and engaging to the target audience.

Furthermore, the success of the game in other European countries would depend on the availability of suitable infrastructure and resources. This includes having access to reliable internet connections, adequate computer equipment, and trained educators to facilitate the game. Therefore, it is important to ensure that the necessary infrastructure and resources are available before launching the game in other countries.

In addition, collaboration with local partners and stakeholders is important in ensuring the success of the game. This includes engaging with schools, educational institutions, and government agencies to promote the game and ensure its integration into the educational curriculum. By working closely with local partners, it is possible to identify and overcome any barriers or challenges that may arise during the implementation of the game.

4 Marketing & dissemination

When conducting a project, it is important to consider the replicability and exploitation of the results obtained. Dissemination of the project's outcomes through various channels is critical to achieving these goals. One effective approach is to create different dissemination materials, including written and video content. Written materials such as reports, articles, and blog posts can provide a detailed explanation of the project's objectives, methodology, and findings. Videos, on the other hand, can offer a visual representation of the project's progress and outcomes, which can be easier to understand for some audiences. By using a combination of written and video materials, project teams can better disseminate their results and increase the chances of replication and exploitation by others.

Within the Cyber4Schools project we have produces several different dissemination, and as well educational material. First group of those material are written reports related with the cybersecurity topics:

Written (intellectual outputs) materials:

1) [Training Path of the online course for teachers on cybersecurity and game application in schools](): document explaining and defining the structure/"articulation" of the course that contain a description

of the training stages and the training units necessary to train the selected teachers to become peer trainers/facilitators in the field of digital security for secondary school pupils, able to support their counterparts during the implementation of the CYBER4SCHOOLS Game. This document might be also helpful for other who wants do develop their own game.

2) Training kit for the online course for teachers on cybersecurity and game application in schools, this document is divide into two part:
    a. Teacher's training kit
    b. Guide on Cyber Security

3) Training path of the game on digital security for secondary schools pupils: document explaining what was the roadmap for the creation of the cyber security lessons (modules) and game scenarios (including the description of them).

4) Training kit for the game implementation for secondary schools pupils: a set of different materials for all lessons:

    a. Lesson 1 – Cybersecurity theory
    b. Lesson 2 – Cyber4Schools: pre-game
    c. Lesson 3 – Cyber4Schools: game playing
    d. Lesson 4 – Wrap up after the game

These material contains of power point presentations, printed materials, readable material etc.

Video materials:

1) Promotional video
2) Cyber4Schools Portal Login Guide
3) Game tutorials:
    a. Episode 1: Phishing – Blue Team
    b. Episode 1: Phishing – Red Team
    c. Episode 2: Malware – Blue Team
    d. Episode 2: Malware – Read Team
    e. Episode 3: Network security – Blue Team
    f. Episode 3: Network security – Red Team
    g. Episode 4: Password security – Blue Team
    h. Episode 4: Password security – Red Team
    i. Episode 5: Web application security – Blue Team
    j. Episode 5: Web application security – Red Team

All material that are available on our project website, YouTube channel and C4S game portal, are available at least till April 2025.

5 Conclusions

In conclusion, the cybersecurity training programme developed within Cyber4Schools project has the potential to be a highly effective tool in educating individuals and organizations about the importance of cybersecurity. Through its emphasis on interactive learning methods and gamification, the program provides a fun and engaging way for individuals to learn about cybersecurity basics and best practices.

Moreover, the training programme's modular design and adaptability make it an excellent platform for further development and adjustment to different circumstances. This adaptability means that it can be tailored to suit the specific needs and interests of a wide range of end-users, from schools and educational institutions to businesses and public sector organizations.

One standout feature of the program is the Cyber4Schools game, which provides a highly interactive and immersive experience that can be used to reinforce the key cybersecurity concepts covered in the program. The game offers a unique opportunity for individuals to put their knowledge into practice and learn from their mistakes in a safe and controlled environment.

Overall, the training programme and the Cyber4Schools game represent a valuable resource for anyone looking to improve their knowledge and skills in cybersecurity. As the importance of cybersecurity continues to grow in our interconnected world, the need for effective training and education in this area will only become more pressing. The program's adaptability and flexibility mean that it can be used by a wide range of stakeholders and end-users, making it a highly valuable and versatile tool for promoting cybersecurity awareness and education.