Co-funded by
the European Union

EyesOnCS
Cyber Alert Scenarios

English
December 2023

Projektdaten

Acronym:	**EyesOnCS**
Title:	**Enhancing Cyber Security – Development of trainings using "Escape Room" Model**
Project No.:	2021-1-DE02-KA220-VET-000033003
Duration:	01. January 2022 – 31. December 2023 (24 months)
Programme:	Erasmus +, Key Action 2: Cooperation partnerships in vocational education and training
Projekt Lead:	Fachhochschule des Mittelstands (FHM)
Issue:	December 2023

Participating project partner organisations

Staatlich anerkannte, private
Fachhochschule des Mittelstands (FHM)

virtualcampus

AKADEMIE ASW

fb
finance & banking
Associazione
per lo sviluppo organizzativo
e delle risorse umane

Stay tuned!

Follow us

Find out more about the project here:

www.eyesoncs.eu

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Contents

1 Summary

This document is a product of the ERASMUS+ project EyesOnCS, aimed at developing and testing a virtual training for in-company training and vocational education in the cyber security field based on real cases and requirements. The project focused on implementing an innovative Educational Escape Room (EER) approach. The development of learning scenarios, serving as the foundation for scenarios and episodes, is outlined in this report.

The initial section of the report summarizes pedagogical concepts from the literature and their application to the project's objectives. It discusses the advantages and limitations of gamification in the didactic process, emphasizing the need for further research on the long-term effects of gamification and EERs on learning quality. The EyesOnCS project aims to contribute to this area by exploring various digital methods in vocational training, with a focus on game-based learning of CS content using the Escape Room Model.

The subsequent chapter outlines the methods and principles for developing learning scenarios, and learning objectives. Practical methods for deriving learning objectives from real-life cases are discussed, leading to the definition of general learning objectives, including expanding knowledge of cyber-attack methods, enhancing security awareness, acquiring knowledge of behavioural principles used by cybercriminals, and recognizing the potential criminal use of social media.

In the fourth chapter, six detailed learning scenarios are presented and mapped to game scenarios or episodes: "The Test," "The Job," "The Hacker," and "The Expert." These scenarios, derived from practical investigations, cover topics such as identity theft, CEO fraud, social media and passwords, and phishing scenarios. Each learning scenario is associated with specific learning objectives, information on protection against attacks, and implementation potential within the game episodes.

Overall, the main outcome of this project phase is the development of four implementable game scenarios for an EER educational game based on six learning scenarios derived from practical investigations.

2 Introduction

The issue of computer security and cybercrime has grown increasingly critical worldwide in recent years, driven by several factors. One significant factor is an increasing use of potentially vulnerable computers and networks for the exchange of sensitive information. Attacks on these systems, as well as their improper use, cause a substantial harm on individuals and organizations. For instance, the German computer industry association Bitcom reports damages exceeding 220 billion Euros annually. For small and medium-sized enterprises, such attacks and the theft of commercial sensitive information can spell economic disaster (Streim & Mann, 2021).

The recent coronavirus pandemic has aggravated this problem, particularly with the adoption of new internet-based work formats. Protective measures have often lagged or failed to adapt promptly. During the pandemic, remote work and network-based communication have created new ways for intruders and cybercriminals to exploit the security vulnerabilities of both businesses and private individuals. This concerning trend shows no signs of abating. To provide context, the reported damages in 2018/19 amounted to approximately 103 billion euros.

Hence, it is paramount to educate both employees in companies and private individuals about the consequences of cyberattacks, as well as effective defence strategies, to heighten their awareness**.** **Internal and external training**, therefore, emerges as **a key factor** in safeguarding against cybersecurity threats, with Higher Education Institutions (HEIs) assuming an increasingly vital role in this process.

The ERASMUS+ project "EyesOnCS" was dedicated to enhancing in-company training in the cybersecurity domain using game-based methodologies. The present document compiles the game scenarios to be implemented with a Cyber Security (CS) training using the Escape Room Model.

Major objectives for this report are:

- Brief description of the underlying pedagogical concepts for scenario/game-based CS learning for an escape room game application,
- Specification of learning objectives of the scenarios,
- Derivation and documentation of appropriate escape room game scenarios to be implemented.

The fulfillment of the goals and tasks is envisioned through a structured approach, incorporating various essential elements. The document involves pertinent pedagogical concepts extracted from scientific literature, ensuring a solid foundation for the educational framework. Six distinct sets of situations have been created to diversify the learning experience and cater to a broad spectrum of scenarios.

For all scenario learning objectives were shaped to specify the knowledge and experiences learners acquire, gain, and possess upon completing the learning process. This ensures a tailored and focused approach, aligning with the specific goals of each scenario. The definition of appropriate scenario situations for each individual scenario explores diverse contexts and are adapted to the Escape Room. The Escape Room approach as a scenario framework provides an immersive and engaging structure for the learning experience, enhancing participant involvement and comprehension. The final steps involve the detailed drafting, phrasing, and documentation of the game scenarios.

This document presents six different cybersecurity scenarios, which amalgamate real cases outlined in IO1 (EyesOnCS-Team, 2022). The real-world cases showcased in IO1 were selected from three EU partner countries and serve as a collection of ideas for learning scenarios. The scenarios developed and compiled in this document were incorporated into the final Escape Room game IO3 and adapted to enhance gaming experience and usability.

The scenarios outlined in this report IO2 illustrate prevalent and deceptive cyber threats, including phishing, voice phishing (vishing), CEO-Fraud, smishing, password security, and social engineering. Through exploring these complex subjects, the aim is to comprehend the intricacies of each attack vector and devise innovative countermeasures to mitigate their impact. Accordingly, the scenarios immerse players in various roles such as a CISO (Chief Information Security Officer), white hacker, or individual tasked with creating an awareness campaign.

Each scenario comprises at least three subparts. The first part presents the scenario itself, depicting a plausible situation in which the player may find themselves during work or in their personal life. Initially, the player is confronted with an attack method/vector, as described in the preceding paragraph. Additionally, suggestions are provided regarding possible actions or decisions the player could take within the game. Following the scenario description is an explanatory segment, detailing the current attack method in depth. This may include a brief explanation of typical psychological behaviours or the utilization of specific tools.

The second part of each scenario briefly outlines the learning objectives targeted within the scenario. Each scenario concludes with a third section offering advice on how players or users can protect themselves against the cyber threat presented in the scenario, supplemented by implementation notes.

3 Theoretical overview

3.1 Pedagogical and didactic concepts

To establish educational game scenarios that are both useful and effective, a robust pedagogical didactic concept is essential. This chapter aims to provide a scientific background, addressing the following key questions:

What pedagogical concepts are,
What didactic concepts are and what kind of such concepts do exist,
Which didactic might be applied,
Why we decided to employ game-based learning as main didactic concept,
Why we decided in favour of the "Escape Room" model as a didactic game concept.

A pedagogical concept involves educators assuming full responsibility for guiding the student learning journey. Teachers leverage students' prior knowledge to facilitate skill and knowledge development. The primary aim of a pedagogical concept is for educators to help students grasp the subject matter by understanding their unique learning styles. Educators set the pace of learning by breaking down the subject matter into manageable units (topics) and assess students' progress through critical thinking evaluations. Upon completion of the curriculum and successful assessment, students can advance to a more advanced level of the subject (Owa, 2022).

Pedagogical concepts encompass didactic concepts, and this report aims to present both in order to effectively impart cybersecurity knowledge to students. Didactics and pedagogy are closely related with education and instructional methodologies, though they carry nuanced differences. While often used interchangeably, they possess distinct meanings.

Didactics specifically refers to the science and art of teaching, which includes methodologies such as gamification. It emphasizes the principles, techniques, and methods of instruction, embracing the design, development, and delivery of educational content to facilitate effective learning. Didactics involves considerations of learner needs and characteristics, selection of appropriate teaching strategies, and organization of instructional materials and activities.

Pedagogy, as a broader concept, contains the theory and practice of education, including the strategies, approaches, and methods employed in teaching and learning. It considers the comprehensive educational context, which involves aspects such as the learning environment, curriculum development, assessment techniques, and the social and cultural factors influencing learning. Pedagogy revolves around understanding how learners acquire knowledge, skills, and attitudes, and how educators can effectively facilitate their development.

In contrast, didactics focuses more specifically on the techniques and methods of teaching, honing in on instructional strategies and methodologies. While didactics delves into the practical aspects of teaching, pedagogy provides a broader philosophical framework for educational practice.

Both didactics and pedagogy share the common goal of enhancing the learning process and fostering meaningful and effective instruction. They require educators to understand learners' needs, employ appropriate teaching strategies, and cultivate an engaging and supportive learning environment. These concepts serve as essential foundations for educators striving to achieve optimal teaching and learning outcomes (Mugambi, 2021).

The term "didactic concept" is frequently used interchangeably with "didactic method" in academic literature. A didactic concept or method refers to a teaching approach that consistently applies scientific principles or educational styles to deliver information to students. This instructional method is often juxtaposed with dialectics and the Socratic method. It can also denote a specific didactic approach, such as constructivist didactics (Wikipedia, 2022).

The theory of didactic learning methods centers on students' foundational knowledge and aims to enhance and convey this information effectively. It establishes the basis or starting point in a lesson plan, with the overarching objective being the acquisition of knowledge (in this case, cybersecurity knowledge). In this role, the teacher or educator serves as both an authoritative figure and a guide, providing support and resources to students. In certain contexts, the teacher's role may be assumed by an avatar or even automated algorithms within a game environment.

Constructivism, often cited as the theoretical underpinning of didactic concepts, emphasizes learning through simulated scenarios, fostering discovery learning and creative engagement with software tools, such as configuration tasks. Common didactic approaches include the traditional "demonstrate - imitate" method and "task-based learning." Additionally, the playful integration of game elements, known as "gamification," is increasingly recognized in educational literature (Goertz et al., 2021).

In the EyesOnCS project, the focus is put on the constructivist didactic concept of gamification. This concept originated in 2002 with consultant Nick Pelling, who introduced playful hardware enhancements on his website. This principle involves integrating gaming elements into non-gaming environments. Gamification labels a phenomenon that predates the current gaming industry and the widespread use of the term, having already emerged in marketing practices (Gajanova et al., n.d.).

3.2 Gamification in Education

Numerous studies support the positive impact of gamification in both education and marketing (Plessis, 2011). This can be attributed to the innovative utilization of user knowledge in progressive marketing communication, enabling companies to gain a competitive edge. Currently, gamification is emerging as an innovative approach in vocational education.

Between 2011 and 2013, gamification quickly rose to prominence as a concept in information technology trends, highlighted by its inclusion in the Gartner Hype Cycle. However, the latest iteration of the Gartner Hype Cycle has challenged this notion, placing gamification in the "Trough of Disillusionment" alongside hybrid clouds and augmented reality. Nevertheless, there are compelling reasons to view gamification as a promising trend for the future.

Firstly, the continually evolving gaming industry suggests ongoing potential for gamification. Secondly, the proliferation of smartphones and wearable technology, coupled with the trend of Self Information via Mobile and Wearable Devices (Rawassizadeh et al., 2015), which involves collecting and accessing personal data through smart devices, creates fertile ground for gamification to thrive. Therefore, gamification seamlessly complements these advancements. These developments have sparked discussions about the practical utility of gamification, particularly in vocational training. Consequently, an increasing number of Educational Institutions are integrating gamification into their educational processes.

The currently accepted definition of gamification, as proposed by Caponetto et al. (2014), is:

Gamification is the use of game elements in a non-game environment.

Game elements must establish specific rules or a structure to motivate or support participants' actions, particularly in vocational Cyber Security training. In the realm of educational processes, definitions of gamification often diverge from general attempts to define it. Gamification serves to inspire learner participation and interaction in activities. In this educational context, gamification can be described as an effort to alter thinking styles and employ game rules in a manner that enhances motivation to solve problems (Gajanova et al., n.d.).

The objective of gamification is to motivate and engage learners while offering feedback that amplifies student involvement, interest, and motivation to learn. Didactic form refers to the organizational framework of teaching and learning, encompassing various methods of managing and structuring the educational process.

In this context, gamification aligns closely with this approach, resembling it from a game design perspective. It is characterized as internal and systematic, comprising interactive, interconnected, and interdependent elements that together form a complex unit (Salen & Zimmerman, 2003).

Comparing the definitions of didactic form/method and gamification reveals a significant overlap between the two concepts. Consequently, it can be inferred that gamification does not conflict with the didactic form. Instead, due to its diverse range of tools and direct elements, gamification can be viewed as an adaptable tool within the didactic framework, capable of influencing and responding to individual management methods and elements of the organizational teaching framework. Gamification is inherently connected with education and serves as a potent didactic tool. Its effectiveness stems from its foundation in motivation and the enjoyment of learning. Therefore, it should be embraced as an integral component of educational practices.

With the advent of modern Internet technology, virtual reality, and artificial intelligence, traditional teaching methods are increasingly perceived as uninteresting and often ineffective. Depending on how gamification is implemented, particularly in Cyber Security (CS) training, it can significantly impact students' learning success, engagement, and motivation. The integration of gamification into continuing education, as well as across all other educational domains, is advantageous and therefore essential. Hence, it's unsurprising Education Institutions are actively seeking ways to enhance the vocational education system through gamification.

According to Google Trends, over the past five years, the most frequently searched queries related to "gamification" were terms like "gamification education" or "gamification in education." This underscores the need for gamification in Vocational Education and Training (VET). However, these areas present challenges as they are not easily gamified, and not all gaming tools can be effectively utilized (Marczewski, 2015). Thus, there is a pressing need to explore new approaches to educational gaming.

The EyesOnCS ERASMUS+ project is focused on pursuing this strategy, aiming to innovate and improve educational gaming experiences in the field of CS training.

// Advantages of Gamification in the didactic process

Several authors advocate for the use of gamification in the didactic process, citing various advantages. This stems from the notion that players within a specific game form a unique community where they collaborate, strategize, and engage in substantial intellectual work together. As they progress through levels or episodes of the game, they naturally transition to increasingly challenging tasks, mirroring a classic learning curve. Players, or students, derive enjoyment from accomplishing progressively difficult goals (Squire, 2011).

Proponents of gamification primarily emphasize the technical game mechanics, which serve as the fundamental building blocks of games. This gaming experience presents a compelling alternative to the traditional teaching system.

The primary advantage of educational games, particularly in vocational training, lies in providing students with opportunities to test and practice new skills, as well as to challenge one another.

However, the objective isn't solely to directly integrate the game with learning, such as in the context of Cyber Security. Equally important is the ability for students to apply the acquired knowledge into real world, such as their professional roles within a company, facilitated by the game. Gamification enhances learners' engagement, particularly with topics that may initially lack appeal. Through task-specific design, gamification reinforces learning outcomes, underscores achievements and progress, encourages better performance, and fosters collaboration and knowledge exchange within the group (Gajanova et al., n.d.).

Presently, the international scientific community is collectively convinced of the benefits of gamification in the didactic educational process (Becker & Metz, 2022). In the context of the current ERASMUS+ project, gamification involves gaining points, receiving immediate feedback, and overcoming challenges, as outlined in Chapter 4. Collaborations with other universities have shown an increase in the study success rate from 82% to 95% (Bernardes et al., 2022). These results indicate that the application of gamification not only fuels students' motivation but also enhances their knowledge. Furthermore, gamification assists weaker students in achieving better results.

// Limitations of Gamification in the didactic process

Similar to other well-known didactic methods aimed at supporting teaching, gamification also possesses limitations and weaknesses in the educational process (Mugambi, 2021). Several authors have highlighted the disadvantages of gamification in education. For instance, they note that certain pre-programmed steps and expected solutions to problems may restrict performance expectations (Werbach & Hunter, 2020). This limitation is akin to the priming effect often observed in questionnaires, where tasks and answer options may subtly influence respondents towards a specific response or solution.

One criticism is that learners may not be encouraged to develop their own creative solutions to problems, but rather conform to the expectations set by the game's designers. However, this concern can be mitigated through individual support from the educator outside the game environment and through ongoing development of the gamified learning environment.

The pre-programmed nature of lessons is perceived as a limitation of gamification in education as it may restrain learner´s natural joy of discovery. However, in reality learners have a significant degree of freedom within gamified learning environments. This approach resembles the well-known heuristic problem-solving method, wherein students actively engage in the search for and discovery of knowledge. They are encouraged to analyse and understand problem solutions to apply similar procedures to solve similar problems in the future. One drawback of this method could be the time required, as each learner works individually and solves problems at their own pace (Gajanova et al., n.d.).

To reiterate the issue, particularly in the context of the EyesOnCS project, the long-term effects of gamification on learning quality have not been sufficiently investigated. The EyesOnCS project aims to address this gap with contributions. Gamification in education, especially in continuing vocational education and training, is a multifaceted and fragmented topic. The authors lack specific references regarding the use of game-based learning in Cyber Security. Some general studies have yielded conflicting conclusions (Richter & Müller, 2023). For example, a history-based game enthused students but led to a decline in their knowledge retention (Hammer & Black, 2009).

Studies on the effectiveness of gamification with younger learners have shown that it neither optimizes nor impairs study results (Rachels & Rockinson-Szapkiw, 2017, cited in Gajanova et al., n.d.). However, other findings have demonstrated a positive effect of challenging games on learning effectiveness, albeit limited to intensive gamers. The effectiveness of the escape room approach chosen for the EyesOnCS project in the realm of Cyber Security further education remains an open question. The subsequent report on the implementation and testing of the escape room game is expected to shed light on this matter (EyesOnCS-Team,2023).

3.3 Gamification and game-based learning

To gain a better understanding of the format's implications, this project will focus on game-based learning and serious games.

Digital game-based learning refers to educational methods utilizing computer games, virtual worlds, and similar platforms. The term "edutainment," derived from "education" and "entertainment," encompasses the integration of learning and entertainment elements across various media, including computer games. Users primarily engage in practicing previously learned skills (Albrecht & Revermann, 2016, cited in Richter & Müller, 2023).

Serious games are computer games designed not only for entertainment but also to address more significant purposes or backgrounds. These games utilize technologies commonly found in entertainment software but serve applications beyond pure entertainment. Serious games incorporate elements such as game ideas, rules, action situations, and tension-inducing elements. The focus is on gameplay to enhance learner engagement within a specific learning context, promoting motivation and facilitating longer-term retention of acquired experiences (Albrecht & Revermann, 2016, cited in Richter & Müller, 2023).

Advantages of game-based learning	Disadvantages of game-based learning
• playful addition to various teaching methods	• learning content is (partly) subordinate
• trend towards high motivation potential among learners through a sense of achievement in the game (increased intrinsic motivation)	• requirements for technical equipment vary-(high) (investment) costs for acquisition and ongoing

• opening up scope for action through interaction	• target group-specific games on the market are few/very differentiated
• appealing design	• high need to check the usefulness and appropriate use in the learning process
• active participation is necessary for shaping the game and can be tracked	• prior knowledge of teaching staff required
• promotes sustainable engagement with learning content	

(Richter & Müller, 2023)

Experiential learning forms the foundation of game-based learning, emphasizing the process of learning through hands-on experiences. By actively engaging learners in practical activities and subsequent reflection, they can effectively bridge theoretical knowledge gained in the classroom with real-world situations. Escape Games, an Innovative Approach for Didactic Concept and Learning Method," exemplify experiential learning in action. This approach enables players to experiment and explore within a safe environment provided by the game.

Gamification vs. game based learning and learning by gaming:

Gamification involves integrating game elements such as levels or experience points into standard learning routines to incentivize students to meet expected behaviours through rewards. On the other hand, (video) learning games are typically designed solely for educational purposes - which poses their primary challenge: Their focus is often on acquiring factual knowledge and may lack the engaging gaming principles that make "authentic/real" video games so compelling (Wössner, n.d.).

In contrast, the goal of game-based learning is to transform the learning experience to align with the world in which young people live. Game-based learning incorporates popular (classic) games like Minecraft or specially developed games such as the EyesOnCS Escape room. Instead of exactly planning each lesson to be delivered according to a fixed curriculum, educators design projects in which learners engage with the chosen game to achieve educational objectives.

Another emerging approach, learning through gaming, has been increasingly regarded as a futuristic idea. This concept is often showcased at events like edu-game jams, where teachers collaborate with programmers and sometimes young individuals to develop video game prototypes. These prototypes facilitate skills-oriented learning and incorporate gaming principles that have contributed to the success of many traditional games. During gameplay, learners acquire knowledge that they must then apply in an action-oriented manner, sometimes through a transfer, to progress in the game.

This project focuses on escape games, which are designed to enhance problem-solving skills and, depending on their structure, enable learners to practice one or more of the 4Cs (communication, collaboration, creativity, critical thinking). Typically, participants are either confined in a space and must solve puzzles to unlock the door (EyesOnCS-Team,2023), or they encounter a locked box that they attempt to open. Escape games are often immersed in an engaging narrative framework, which may or may not be directly related to the specialized or skill-based puzzles presented.

As previously mentioned, at the start of the EyesOnCS project, the project team opted to utilize game-based learning as the primary didactic concept for conducting vocational training in Cyber Security. Specifically, the focus is on serious games.

On one hand, video games, which emerged as consumer products roughly half a century ago, have undergone significant evolution since their inception as mere leisure activities. They have evolved into integral components of social and cultural landscapes, exerting a substantial influence and presence in society across various domains. The journey began with simple games like Pong (a form of tennis game) in the 1970s, initially developed in garages or basements. The evolution of gaming progressed through the years, culminating in the production of AAA titles with budgets reaching up to 300 million dollars by 2023 (Warby, 2023).

According to Goertz et al. (2021), these interactive mediums have evolved beyond mere entertainment to become deeply integrated into modern culture. Games, as inherently endogenous systems, consist of structured problem-solving activities governed by specific mechanics and rules. These elements collectively foster engagement, with players participating out of internal motivation. Gameplay dynamics, the core of these systems, facilitate diverse interactions between players and game elements, leading to varied behaviours and outcomes. This interaction is crucial in fostering a sense of immersion, described as deep mental involvement by Agrawal et al. (2020). Players' evaluations of choices within games not only enhance their immersion but also significantly contribute to socialization, critical thinking, and logical reasoning. Furthermore, games play a vital role in refining cognitive, intrapersonal, and interpersonal skills, including perceptiveness, attention, memory, and various analytical abilities.

The evolution of video games has extended beyond entertainment. Recognizing the motivational and engaging aspects of gameplay, designers have repurposed these attributes, particularly for educational and training purposes.

These applications, also known as "serious games," are primarily designed not for entertainment but to leverage the inherent motivation and immersive experience of players. They employ effective game mechanics to impart skills, knowledge, and awareness in an entertaining environment, often used for educational purposes.

On the other hand, the education sector, in particular, has witnessed significant success with the integration of serious games, giving rise to the concept of "game-based learning." In this approach, games are developed with explicit learning objectives, as done in the present Cyber Security courses, enabling learners to gain experience in their respective fields of study within a controlled environment. Such games promote the development of skills and competencies, enhancing social skills, teamwork, leadership, and collaboration.

As noted by Prensky (2005), game-based learning combines the engaging aspects of gaming with educational content, creating an interactive learning experience that motivates users to explore and deepen their knowledge. Abt (1987) outlines the benefits of educational games, emphasizing their role in problem-solving introduction, alignment of game objectives with educational goals, promotion of understanding abstract concepts, fostering critical thinking, providing real-time feedback, and offering safe environments for exploring consequences and authentic assessment. Additionally, serious games have proven beneficial in training for hazardous processes, such as Cyber Security applications and training, or situations where physical classrooms are impractical or expensive.

In the realm of vocational training, the theoretical concepts of video games have found a niche through gamification, a method that integrates game elements into non-game contexts to enhance user engagement, productivity, and motivation. As discussed earlier, gamification has proven particularly successful in training and development programs, where interactive, game-like simulations aid learners in acquiring new skills and knowledge within a more engaging and less formal environment, especially in fields like CS training. This innovative application of gaming principles in education underscores the versatility and adaptability of video games as tools for engagement across various settings (Goertz et al., 2021).

Therefore, the fundamental didactic concept of this project revolves around experimental, game-based learning of CS content within the realm of vocational training.

So why experimental Cyber Security learning? The answer is quite straightforward, as highlighted by (Nationale Agentur, 2021)

- Real-life experiences: Players are immersed in real-life scenarios that mirror daily occurrences when working with a computer connected to the Internet. Moreover, there's a merging of Internet usage between office work and daily life.
- Immediate perception of consequences: During the gaming experience, learners can make decisions within a safe space where they can observe the direct consequences of their actions. This facilitates experiential learning and deepens understanding. Learners can witness potential consequences such as identity theft or credit card fraud.
- Practical actions leading to better understanding: By engaging in realistic scenarios, learners can take practical actions that contribute to a better understanding of the subject matter.
- Improved knowledge retention: The immersion in gameplay and immediate feedback on consequences directly enhances knowledge retention, as learners experience and learn from each decision and its outcomes during gameplay.

Through the experiential and game-based learning approach, educators and learners can tailor training formats to suit the needs of non-technical staff or learner in VET. This approach empowers learners with an active, self-directed role, incorporating realistic situations encountered in everyday working life. For instance, in EyesOnCS relevant situations encompassing areas such as Cyber Security, phishing, remote work, social media, etc., are combined into a series of six different scenarios. These scenarios integrate standard and challenging situations, along with learning objectives.

3.4 The “Escape Room Model” as innovative approach

An "escape room" is an interactive game where a team of players works together to discover clues, solve puzzles, and complete tasks within a set time limit to achieve a victory goal. These games take place in various fictional settings such as prison cells, dungeons, laboratories, or space stations, depending on the chosen theme, with the players' objectives and challenges aligned accordingly. The game typically begins with a brief introduction to the rules, provided through video, audio, or by a live gamemaster. Once inside the designated room or area, a countdown timer starts, usually set between 45 to 60 minutes, which limits the time available to complete the game. Players then explore the space, searching for clues and solving puzzles to progress further.

The challenges in escape rooms are predominantly mental rather than physical, requiring different knowledge and skills for various types of puzzles. If players encounter difficulties, they may request hints, which can be provided in written, video, or audio form, or directly by a live gamemaster.

The game concludes either with a successful outcome, such as escaping "alive" within the time limit, achieving the room's objective, or thwarting the story's threat or antagonist, or with an unsuccessful outcome, such as being "killed" by the main antagonist or facing consequences once time runs out. Aside from entertainment, escape rooms also serve as platforms for promoting collaboration, teamwork, and team building among participants.

Virtual, digital, or online escape rooms are digital equivalents of physical escape rooms, conducted through computers and networks. Players, whether individuals or teams (such as learners), communicate and collaborate via synchronized online platforms like Zoom or specially developed game interfaces, as seen in the EyesOnCS project. Game software is utilized, allowing for single-player or team-based gameplay over the network. Similar to physical escape rooms, players in virtual settings solve riddles and puzzles within a predetermined time frame. More advanced digital escape rooms may incorporate virtual reality technology to enhance player immersion.

In recent years, the academic and vocational training sectors have recognized the educational benefits of escape rooms and have begun incorporating them into their programs. Although research on educational escape rooms (EERs) in Europe is still developing, there is a growing body of scientific studies examining their effectiveness and applications (Tercanli et al., 2021). This project aims to contribute to this research.

Educational Escape Rooms are utilized at various stages of the learning process. Some EERs are designed for beginners with no prior knowledge, allowing participants to acquire foundational concepts, while others are tailored for those with existing knowledge, providing opportunities for deeper learning through specialized teaching approaches. (Tercanli et al., 2021), (Guckian et al., 2020).

Various studies analysed during the initial phase of the EyesOnCS work package "Definition of learning objectives (IO2/A2)" have demonstrated that both offline and virtual Educational Escape Rooms (EERs) are effective learning methods. This finding is supported by a significant increase in learners 'knowledge following their participation in EERs. On average, students experienced a substantial 53% increase in knowledge (Euckel et al., 2020). Additionally, it was observed that students retained the acquired knowledge better after engaging with EERs (Brady et al., 2019). Therefore, EERs not only contribute to enhancing the level of knowledge but also serve as a unique pedagogical tool that can stimulate students' interest in science and technology.

The prevailing literature consistently supports the notion that participation in Educational Escape Rooms (EERs) increases learners' interest in the covered topics. The EyesOnCS project team aligns with this perspective for teaching in the field of Cyber Security (CS) and advocates for EERs as the preferred method for implementing the didactic approach of "Game Based Learning". According to existing literature, EERs are regarded as a valuable educational method. EERs not only facilitate a deeper understanding of the course material but also encourage students to discern connections between various topics (Brady et al., 2019). Moreover, research indicates that EERs positively impact students' confidence, both academically and in the practical application of their knowledge. Evidence showing a significantly higher pass rate on exams underscores the beneficial learning effects of EERs. Additionally, EER activities assist students in comprehending a broader perspective of course material by elucidating additional interrelationships between topics (Brady et al., 2019; Tercanli et al., 2021).

The escape room approach fosters the development of soft skills, notably enhancing motivation and refining abilities such as problem-solving. Through Educational Escape Rooms (EERs), participants are also encouraged to cultivate team-building skills, embrace out-of-the-box thinking, and engage in critical questioning. Beyond these varied skill sets, learning through the escape room method also cultivates awareness of specific topics, which is particularly advantageous for the current project's objectives. The project aims to promote awareness of responsible practices in handling CS issues. Therefore, EERs serve as a highly effective learning method, substantially enhancing participants' knowledge and consciousness. (Tercanli, H. et al., 2021).

It can be assumed, that the escape room model approach holds significant potential for enhancing further training in Small and Medium Enterprises (SMEs). Through the EyesOnCS Escape Room training for Cyber Security awareness for the topic can be raised among the (non-technical) employees. The fundamental concepts of CS will be presented to foster a sense of security through playful learning. The goal is to create the most efficient learning curve possible, particularly in a field like CS that may be unfamiliar to some individuals.

The integration of scenario-based learning with a game-based implementation of the Educational Escape Room (EER) model proves highly effective for learning. This combination offers a realistic context alongside an emotional connection, thereby boosting motivation and expediting skill acquisition. For the EyesOnCS project, this approach is preferred for its ability to enhance learning objectives. In the realm of Cyber Security, referencing realistic situations can significantly enhance learning outcomes, enabling learners to better grasp and apply concepts in their professional environments.

The creation of the scenarios using the EER model for imparting knowledge for non-technicians in the field of Cyber Security pursue following objectives and effects (Nationale Agentur, 2021)

- Providing evaluated and content-tested scenarios based on the concept of escape rooms for educational purposes in the vocational training sector, as well as for Small and Medium Enterprises (SMEs) seeking to enhance their training activities. This initiative aims to broaden the range of innovative teaching approaches tailored to specific training needs, with open access available to all interested students.

- Assisting learners with limited technical backgrounds in improving their CS skills, thereby empowering them to navigate computerized environments in both professional and personal contexts with greater confidence.

- Facilitating transferability across multiple levels:
    - Horizontally, to various vocational training organizations irrespective of subject area, as cybersecurity has become pervasive across all work environments.
    - Vertically, to other educational sectors such as initial vocational training and higher education, given their shared goal of preparing future employees for computer-based work environments and the associated need for cybersecurity awareness and training.
- Ensuring the scenarios can be adapted for use in diverse educational contexts, providing VET learners with opportunities to practice various realistic scenarios commonly encountered in professional settings.
- Ensuring the scenarios can be translated into real-world applications and spatially reconstructed, reflecting realistic situations that students may encounter in their typical professional environments (Nationale Agentur, 2021).

4 Development of Learning Scenarios

Learning scenarios within computer games represent a dynamic intersection of education and entertainment, leveraging the immersive and engaging nature of gaming environments to facilitate learning experiences. To understand the concept fully, it is essential to explore the definitions of both learning scenarios and game scenarios.

Definition of a Learning Scenario: A learning scenario refers to a carefully crafted and structured sequence of events or activities designed to achieve specific educational objectives within a given context. In the realm of computer games, learning scenarios are created with the intention of incorporating educational content seamlessly into the gameplay. These scenarios often involve problem-solving, critical thinking, and skill development, providing players with opportunities to acquire knowledge or enhance existing skills while navigating the virtual world(Maha et al., 2020).

Usually, learning scenarios are tailored to align with educational goals, leveraging the interactivity and engagement inherent in gaming to deliver content in an immersive and enjoyable manner. They may include challenges, quests, or simulations that encourage players to explore, analyze, and apply knowledge in a dynamic and interactive environment.

Definition of a Game Scenario: A game scenario is the overall narrative or framework that guides the unfolding events and interactions within a game. It includes the setting, characters, plot and objectives that shape the player's experience. Game scenarios serve as the basis for the game's plot and provide the context in which players act and make decisions(Janssens et al., 2014).

Unlike learning scenarios, which are specifically designed for **educational purposes**, game scenarios primarily aim to entertain and engage players. They create a captivating virtual world that encourages exploration, discovery, and the thrill of overcoming challenges. Game scenarios often involve elements of competition, strategy, and achievement, driving player motivation and investment in the gaming experience.

The integration of learning scenarios within computer games represents a powerful approach to educational gamification. By embedding educational content, e.g. content for CS education, seamlessly into game scenarios, developers can leverage the intrinsic motivation of players to enhance the learning experience. This integration fosters active participation, problem-solving, and critical thinking, as players engage with educational content within the context of the game.

Learning scenarios within computer games redefine traditional approaches to education by capitalizing on the immersive and interactive nature of gaming environments. **By linking learning objectives with game scenarios, the developers create a unique and engaging way of learning.** This approach not only enriches the gaming experience but also provides a valuable platform for acquiring and reinforcing knowledge and skills in a dynamic and engaging manner. As technology continues to advance, the potential for learning scenarios within computer games to revolutionize education remains a promising and exciting prospect(Mayer, 2019).

4.1 Derivation of learning objectives from practical cases

Firstly, it is important to define and comprehend the term "learning objective," or ". In the realm of cybersecurity education, learning outcomes and objectives pertain to the specific skills and knowledge that students are expected to attain. These encompass understanding cyber threats, proficiently mastering defence mechanisms (EyesOnCS-Team, 2022), ethical hacking skills, compliance knowledge, and the capability to develop secure systems. Clearly defined learning outcomes in cyber security are indispensable for ensuring that students are equipped to effectively and ethically address real-world cyber threats.

The utilization of practical scenarios in cybersecurity vocational training holds utmost importance in providing learners with hands-on experience in identifying, preventing, and responding to cyber threats. This approach enhances their problem-solving and decision-making skills. These scenarios should be leveraged as instructional tools to replicate the challenges encountered by cybersecurity professionals.

These scenarios should serve as teaching tools to simulate the challenges encountered by cybersecurity professionals (e.g. such as **Escape Room game**). They ought to be grounded in real-world cases encompassing cyber-attacks, data breaches, and defence strategies (For the present project, they are derived from European-selected practical casesEyesOnCS-Team,2022). To ensure alignment between the learning objectives of these scenarios and real-life practical cases, it was necessary to design scenarios targeting specific cyber security skills or knowledge areas. This involved identifying key elements in real-life cases and linking them to educational objectives. For instance, a case study detailing a real ransomware attack (EyesOnCS-Team,2022), could be utilized to teach students about encryption, network security, and legal implications. Similarly, a case involving a data breach could underscore the importance of secure coding practices and compliance with data protection laws.

The development process of these scenarios entailed a thematic analysis: cyber security incidents were analysed to identify common themes such as phishing, malware, or insider threats. These themes were then utilized to formulate the learning objectives for each scenario, aimed at instructing students on how to recognize and respond to these specific threats.

Furthermore, when crafting the learning scenarios, emphasis was placed on experiential reflection. The scenarios are designed to prompt students to critically reflect on their responses to the practical cybersecurity cases and engage in discussions regarding their learnings. This reflective process can subsequently aid in refining the learning outcomes to ensure their alignment with the real-world challenges faced by cyber security professionals.

To develop the EyesOnCS scenarios following steps were carried out:

After analysing 26 real-life cyber security cases from across Europe, as documented in the Compendium (EyesOnCS-Team, 2022), it became evident that the human factor was consistently involved in cyber security attacks, particularly in conjunction with various forms of phishing attacks. Consequently, the EyesOnCS consortium has prioritized addressing this crucial aspect of the prevalent cases and methods of cybercrime documented in (EyesOnCS-Team, 2022). These cyber security attack methods were frequently observed in the investigated cases. However, the consortium has also identified and included new forms of attack, such as smishing.

Upon reviewing the cases, it is apparent that most cybercrime attacks aim to prompt the victim to perform an action while using the computer/smartphone (e.g., opening an attachment, entering confidential data) or deceive them into unwittingly falling into the hands of criminals.

Therefore, the general aims of the learning scenarios encompass:

- Enhancing understanding and knowledge about cyber-attack methods and cybercrime.
- Raising awareness when utilizing internet applications such as the World Wide Web, emails, instant messengers, etc., whether on a computer or smartphone.
- Developing knowledge of fundamental psychological principles and their exploitation by cybercriminals, particularly in social engineering.
- Promoting physical awareness, emphasizing the importance of practices like the clean desk policy and information security.
- Exploring the functions of social media platforms and their potential utilization for criminal purposes.

4.2 Learning flow and scenario storyline

The state of flow is widely recognized as the optimal condition for achieving the best learning objectives. This state, observed in everyday life, entails complete absorption in the current activity, where tasks are tackled with joy and apparent effortlessness. Students in this state become fully engrossed in the task at hand, forgetting their surroundings and dedicating themselves entirely to the activity, which demands their full attention. To enter the flow state, whether during a lecture, group work, educational game, or individual learning, learners simply need to derive enjoyment from the activity. The challenge must strike a balance - demanding enough to require full concentration from the learner, yet not so high as to become overwhelming and lose the sense of ease. The flow experience is bounded by the two extremes of underchallenge and overchallenge (Praxis-Ratgeber Für Bildungsinstitute: Lernspiele in Der Erwachsenenbildung, 2021a).

Motivation plays a key role in achieving flow, with students driven by intrinsic motives to tackle tasks (Tercanli et al., 2021). In other words, what internal factors propel students to engage with tasks? The emphasis is on intrinsic motivation, as it fosters sustainable engagement.

Designers and users of games such as Educational Escape Rooms (EERs) continually grapple with the challenge of maintaining a flow state within the gameplay - striking the delicate balance of providing an experience that is continuously engaging without being overly difficult or too easy. It is often recommended in the literature to conduct timely testing of EER activities to identify and address design and execution shortcomings (Tercanli et al., 2021). This iterative approach allows for continual improvement of the design in subsequent iterations (Friedrich et al., 2020).

A widely used model for understanding intrinsic motivation within gamification is the RAMP model. Gamification involves the application of typical game elements and processes in non-game contexts. The RAMP model identifies four key drivers that explain why students engage in solving tasks: Relatedness, Autonomy, Mastery, and Purpose (Praxis-Ratgeber Für Bildungsinstitute: Lernspiele in Der Erwachsenenbildung, 2021b).

Effective gamification leverages and fosters learners' intrinsic motivation. However, it is important to note that students' intrinsic motivation may diminish over time. To sustain motivation over an extended period, feedback is crucial for students. Various feedback mechanisms, such as awards, assessments, progress indicators, points, or rankings, have been shown to specifically enhance student motivation. These extrinsic factors can also promote intrinsic motivation. Gamification employs these engagement loops (see Fig1) continuously throughout the learning process, serving as the driving force behind gamification.

Learning scenarios play a crucial role in initiating and maintaining flow. The storyline of a game reflects the direction of the learning flow. The term "storyline" originates from the art of storytelling and refers to a dramaturgical story arc. In educational contexts, the storyline method is an action-oriented teaching approach that encourages practical and creative self-activity by learners, often in interdisciplinary lessons.

The pedagogical storyline method emphasizes action-oriented teaching, where learners' practical and creative self-activity takes centre stage in cross-disciplinary training. Learners create their own meaningful representations, such as pictures, models, texts, technical drawings, timetables, and work plans, while engaging with the module. Through these representations, they actively acquire knowledge and skills. This approach aligns with game-based learning principles highlighting the importance of presenting the storyline within the project context.

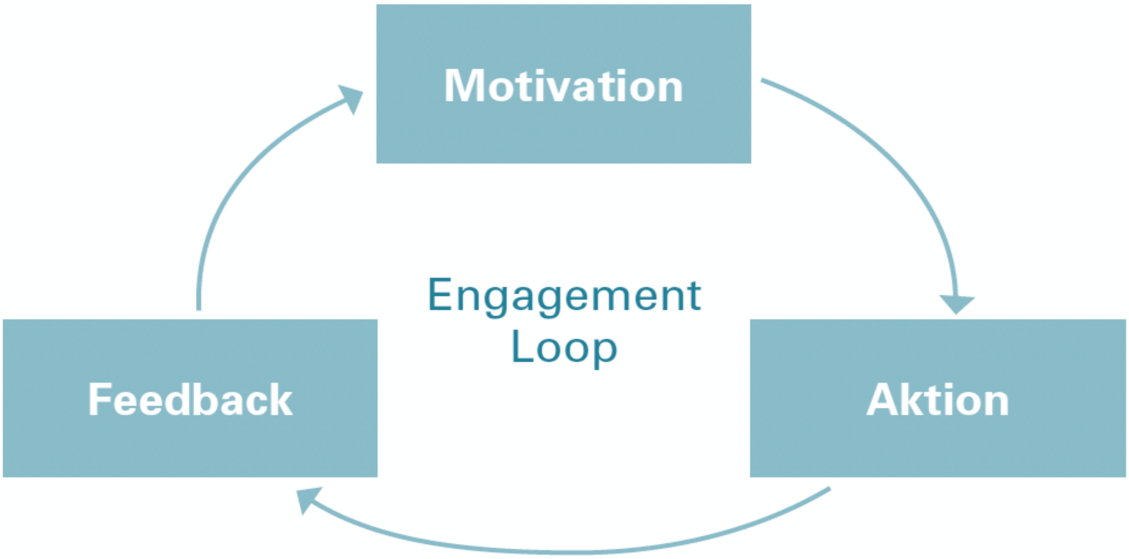


Fig1: Engagement Loop for Gamification (*Praxis-Ratgeber Für Bildungsinstitute: Lernspiele in Der Erwachsenenbildung*, 2021c)

Storyline-based training revolves around a topic that holds significance for learners, drawing upon their ideas and personal experiences. The topic is segmented into chapters akin to a narrative, guiding students through their exploration. For instance, learners may delve into the topic by creating models that unveil previously undiscovered connections. These models should not only be coherent and rational but also aesthetically pleasing. Students' ideas, experiences, perceptions, and assumptions serve as the foundation for their engagement with the topic. Their environment and background experiences provide the groundwork for independent learning.

Behind each training unit lies a narrative, developed gradually over an extended period. Thus, the training follows a thematic thread, hence the term "storyline." Each step along this storyline commences with a key question. The storyline within serious games holds a similar significance for training as evidenced in projects like EyesOnCS. In game-based learning, the game's storyline amalgamates individual scenarios or episodes into a comprehensive educational concept.

4.3 Development of EyesOnCS learning scenarios

Learning scenarios can be categorized using various classification schemes found in international literature. For this project, the scheme proposed by (Goertz et al., 2021) was deemed suitable. This scheme comprises three dimensions with a total of 17 criteria and numerous variables. While some dimensions encompass only a few criteria, others include several sub-dimensions and are thus more extensive. Here, we focus on explaining the three dimensions of technique, setting, and methodology-didactics, along with their associated criteria for practical clarity.

The dimension of "technology" includes criteria selected for systematic examination at the technological level, such as hardware, interaction, navigation, visual fidelity, and sensory perception. The criterion of "visual fidelity," particularly significant in the gaming sector, pertains to disparities in graphical presentation, especially between PC-based applications and those used on standalone devices. Additionally, this criterion evaluates the subjective significance of graphics and appearance. While the influence of these factors on immersion, flow perception, learning experience quality in educational games, or achievement of learning goals is not yet fully understood in many cases.

Another dimension outlined by (Goertz et al., 2021) is the "setting," which encompasses the entirety of content-related and organizational circumstances of the learning scenario. This includes factors like learning support, learning location, target group, learning level, user (group size), type of collaboration, as well as subject matter, topic, and learning content. The criterion of "user (group size)," crucial in the gaming sector, emphasizes the role of group size in categorizing learning scenarios. For instance, while it may be impractical to provide AR glasses for every learner, every learner likely possesses a mobile phone capable of running a computer-based learning game, thus presenting fewer limitations on group size in the latter scenario.

The third dimension, "methodology-didactics", pertains to learning theory anchors, cognitive and affective learning goals (Bloom et al., 1956), and the methods employed. In differentiating scenarios, the learning objectives and the selected method mix are more crucial than the underlying learning theory. Criteria within this dimension include learning theory classification, learning objectives, and didactic methods. The criterion of "learning theory classification," significant in gaming, involves categorization as constructivism, cognitivism, behaviorism, or connectivism. In many practical scenarios, especially in gaming, constructivism serves as a guiding theory, highlighting the approach of various learning projects aiming to initiate autonomous learning processes and harness the explorative potential of augmented reality or learning games (Goertz et al., 2021).

Learning scenarios serve as the catalyst for initiating the learning flow. In the EyesOnCS project, the process of developing game scenarios begins with defining the appropriate situation, guided by the dimensions outlined above (Nationale Agentur, 2021) Drawing from information gathered in previous project steps, such as the development of the compendium (EyesOnCS-Team, 2022), the project identifies gaps in cybersecurity (CS) learning and knowledge. These CS situations are then prioritized based on their real-life significance and likelihood of occurrence in practical or work environments.

Once relevant CS situations from the EyesOnCS compendium are identified, such as phishing emails or safe remote work practices, the next step involves evaluating their potential as effective learning scenarios. Factors like interactivity, experiential and active learning, and the presence of "conflict potential" are considered to ensure student engagement. Revision may be necessary if a situation does not align with the intended learning objectives.

The innovative escape room (EER) model is chosen as a means to raise awareness of CS and train individuals in applying and adhering to relevant CS rules and principles for safe virtual work environments. The EyesOnCS project is pioneering the use of EERs in vocational training, particularly focusing on cyber security as an example. The project aims to discover novel approaches to make learning engaging, interesting, and applicable to real-world work settings.

Cyber security, being perceived as complex and challenging by individuals with limited technical training, also involves an emotional component. Therefore, the EyesOnCS project aims to address these challenges by integrating a storyline into the game-based learning approach, weaving together individual scenarios or episodes into a comprehensive educational concept.

4.4 Learning Objectives and related games

Learning objectives play a crucial role in the effective design and evaluation of an Educational Escape Room (EER) game for VET. Educational institutions, including this project, often rely on Bloom's taxonomy levels (Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. & Krathwohl, D. R., 1956) to guide the development of new courses and define learning objectives. The following *Table 1* illustrates the types of games that align with specific learning objectives. Additionally, the general utility of games in courses, such as in a cyber security, are presented to enhance learning motivation and success.

Bloom's taxonomy levels[1]	Selection of related games
Knowledge	● Various forms of quizzes (online, offline) ● Wall board football ● Various interrogation games (online, offline)
Understanding	● Various quiz forms (online, offline)

[1] (Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. & Krathwohl, D. R., 1956)

	● Wall board football ● Various quiz games such as quartet etc.
Application	● Various quiz forms (online, offline), which are adapted to application examples (example: determining the order of activities) ● Behaviour-oriented games (online, offline): role-playing games like EyesOnCS, etc.
Analysis	● Playful case studies ● Analysis games ● Business games
Synthesis (e.g. solutions development)	● Playful case studies ● Creativity techniques with assessments ● Business games
Assessment	● Mutual solution evaluations ● Assessment games with case studies ● Business games ● Games with jury

Tab1: Relationship between Bloom's taxonomy levels and learning games (*Praxis-Ratgeber Für Bildungsinstitute: Lernspiele in Der Erwachsenenbildung*, 2021)

It is essential to establish clear learning objectives at the outset of the game design process to ensure coherence and purposefulness. The specific objectives will vary depending on the disciplinary field, the level of participant integration, and the game's alignment with the curriculum (Praxis-Ratgeber Für Bildungsinstitute: Lernspiele in Der Erwachsenenbildung, 2021d).

Regarding the EyesOnCS project: Once the topic and areas for the scenarios have been defined, it is imperative to determine the learning objectives. This involves analysing the knowledge and skills learners need to acquire and possess upon completing the learning process. The EyesOnCS project identifies cyber security-specific learning gaps, vulnerabilities, and susceptibilities of the target group (EyesOnCS-Team, 2021) derive learning objectives. Challenging cyber security scenarios, their frequency, and the potential damage and threats they pose serve as references for training and game-based learning. Learning outcomes are formulated individually for each scenario.

Example scenario: VR (Virtual Reality) classroom

As an example from literature, the VR classroom is a training environment for student teachers, in which primarily an adequate reaction to disturbances can be trained. Here, student teachers often take on the role of a teacher for the first time and stand in front of 3D virtual students in a realistic classroom. The VR classroom follows a peer training approach. In the VR classroom, users take on the role of a teacher who is supposed to teach virtual students. The behaviour of the virtual students is controlled by a coach via a web interface, so that the virtual students can start to disrupt or collaborate during the lesson(Goertz et al., 2021).

In this predominantly constructivist example learning scenario, the learning goal of "understanding" and "applying" is supported. In the sense of "adaptive learning" (learning adapted to the learners' current needs), text-based or visual modules are offered as "learning on demand". This can be used excellently for task-based learning and research-development teaching. Gamification would also be possible in this example.

4.5 General reflection on learning objectives and scenarios

Learning applications in the field of cyber security (CS) often share similarities with various general learning scenarios, such as the VR classroom mentioned above. These applications involve activities like interacting with virtual groups, utilizing computers, practicing motor skills (e.g., keyboard typing), navigating unfamiliar situations, and developing social skills. Beyond these objectives, CS applications also aim to instil ethical behaviour and prompt individuals to reflect on their actions. In some instances, they may prompt action to assist others or prevent harm.

Learning objectives, instructional concepts, and the derived scenarios, such as those for learning games, can be highly specific. This has been elaborated in previous chapters of this report. Alongside technical and safety contexts, promoting safe, socially responsible, and ethically sound behaviour is often an affective learning objective. For example, teaching specialized CS-sensitive media skills could be one such objective.

Various instructional concepts are employed in familiar applications (Coughlin et al., 2023; López-Pernas et al., 2019; Mijal et al., 2020), often focusing on concrete actions, sometimes in a playful (gamification) and creative manner. Emotionally charged scenarios, such as employee conflicts where learners must decide on their course of action, are also typical. Task-based learning and targeted reflection are prevalent approaches.

In developing learning objectives for specific CS scenarios (as discussed in the subsequent Chapter 4), the EyesOnCS project team aimed to strike a balance by integrating both technical and non-technical learning objectives for vocational training.

5 The learning objectives for the EyesOnCS Escape Room

Introduction to learning objectives

As mentioned in the previous chapters and required by the project proposal, the general learning objectives for the EyesOnCS Escape Room are the following:

General Learning Objectives for the EyesOnCS Escape Room

- Expanding the knowledge of cyber-attack methods and cyber-crime necessary for professional use,
- Strengthening security awareness in dealing with Internet applications, e-mails, instant messengers, etc. on the desktop computer or smartphone
- Acquiring knowledge of basic relevant behavioural principles and how these are used by cyber criminals, e.g. in social engineering
- Strengthening physical awareness - importance of clean desk policy, information security,
- Recognising important functions of social media and their use for potentially criminal purposes

These overarching learning objectives can be further refined by examining the various attack methods identified by the project team through real cases (EyesOnCS-Team, 2022) and the fundamental knowledge of cybercrime and cyber security. One commonality among all attack patterns is their exploitation of the human factor, where individuals may make errors due to ignorance or susceptibility. The relevant attack vectors identified by EyesOnCS include:

- Phishing
- Password attacks
- Vishing - Voice Phishing
- Smishing
- Social Engineering

The following detailed description will outline the considered attack vectors and their associated learning objectives:

The objectives are outlined as follows:

Phishing: Phishing remains the most prevalent method used by cyber-criminals to infiltrate other computer systems. While precise figures on phishing encounters are challenging to ascertain due to underreporting and varying statistics across countries, phishing emails consistently rank as the primary attack method.

The learning objectives pertaining to phishing for our project are as follows:

- Developing an understanding of typical phishing characteristics in emails.
- Recognizing the basic psychological principles employed by criminals to deceive or manipulate individuals into disregarding security protocols.
- Heightening awareness of the risks associated with unknown data attachments and the divulgence of personal information.
- Understanding the significance of clean desk policies and information security.
- Acquiring knowledge on initial response measures and self-protection protocols.

Password Attacks: Password-related vulnerabilities persist in 2023, with easily guessable passwords like "password1234," birthdays, or relatives' names contributing to account compromises. Weak passwords can be swiftly cracked through brute force attacks. Despite the prevalence of password-related issues, there remains a lack of understanding regarding strong password characteristics. Misinformation further complicates the situation, as seen with outdated advice advocating for regular password changes.

The learning objectives for passwords include:

- Gaining fundamental knowledge about secure password creation.
- Understanding various methods for guessing, cracking, or obtaining passwords illicitly.
- Awareness of clean desk policies.
- Understanding the basics of social engineering on social media platforms to obtain passwords.
- Recognizing the significance of data shared via social media.

Vishing - Voice Phishing: Voice phishing, or vishing, presents a telephone-based variation of classic phishing techniques. Perpetrated by professionally trained criminals, vishing calls aim to extract confidential information or manipulate victims into breaching security protocols. With the emergence of AI voice generators, these tools are now utilized to impersonate CEOs and issue fraudulent instructions over the phone. The learning objectives for vishing encompass:

- Grasping the fundamental principles of social engineering.
- Developing awareness of suspicious call patterns and identifying typical indicators.
- Acquiring knowledge about AI and voice generators.
- Understanding general fraud concepts.
- Learning about initial self-protection measures.

Smishing: Smishing is a variant of phishing and vishing, where attackers use instant messengers or text messages to engage victims in dialogues aimed at eliciting money demands via text. This method is prevalent in both professional and private environments and represents one of the latest cybercrime attack methods.

The learning objectives for smishing include:

- Increasing awareness to identify suspicious text messages.
- Acquiring the ability to verify the authenticity of text messages.
- Developing skills to protect oneself against smishing attacks.

Social Engineering: Social Engineering exploits psychological and behavioral aspects of human nature (Salahdine & Kaabouch, 2019), deceiving or manipulating individuals into disclosing sensitive information or performing actions that compromise security. Nearly every cybercrime attack method is accompanied or supported by social engineering tactics.

The learning objectives for social engineering encompass:

- Developing a comprehensive understanding of the topic.
- Increasing awareness of dangerous messages, emails, and calls from unknown sources.
- Acquiring fundamental psychological knowledge relevant to social engineering.

5.1 Storyline for game scenarios - EyesOnCS Scenarios and Episodes

The presentation of learning scenarios provided the foundational concepts for potential escape room or game scenarios, as detailed in Chapter 3. During the development of the learning game, a blend of these scenarios was utilized, as previously discussed. The planned and subsequently implemented storyline for the EyesOnCS game episodes commences with a fictitious first day at work in a bank. These episodes incorporate various scenarios where the player assumes the role of a new employee in the security department, encountering obstacles aligned with the learning objectives outlined.Each virtual day within the game introduces a new scenario/episode.

On the player's first day, they are tasked with selecting their name and avatar before attempting to gain access to the bank, a challenging endeavor in itself. Subsequent steps include onboarding, logging into an email account, and making initial calls. The player's supervisor is stringent and often threatens termination, frequently contributing to security breaches due to their limited knowledge of cybersecurity. Following the completion of several tasks, the player's role shifts to that of a "white hacker" to provide insight into the attacker's perspective. The storyline culminates with a general quiz on cyber security topics covered throughout the game. Further details on each episode are provided in the following descriptions.

For practical implementation purposes, the original six scenarios outlined below (Scenario 1: Identity Theft via Social Engineering (Vishing) and Phishing of Bank Data) were condensed into four implemented EyesOnCS game episodes. The specifics of the game implementation are not within the scope of this report.

As previously mentioned, the learning scenarios serve as the foundation and source of ideas for the subsequent stages of scape room scenario development. To assist players in completing tasks within the game, information is provided within the game itself or can be accessed via the Internet. In the event of a player becoming stuck, a hint button becomes available after a period, offering a small hint that, depending on usage frequency, leads to the task's solution. The following section briefly describes the four episodes.

Episode 1 - The Test

The first episode commences with the selection of an avatar and the assignment of a name. To gain entry into the new workplace, the player must input an access code, with the initial clue provided by the security guard at the door. The player must creatively combine the letters used for the bank's name, ECS, with the alphabet to derive the access code (5319) for entering the bank. This task, while not directly related to a cyber threat, encourages the player to think innovatively in seeking solutions.

Upon entering the bank, the player is tasked with setting up their email account, including selecting their initial password. Clues around the desk suggest that the chosen password may be incorrect. Once the correct password is utilized, the player is prompted to formulate a new password. Additionally, the player is asked whether they wish to save the password on the computer and whether the antivirus software should be deactivated. The player's response to these prompts leads to further clues regarding the progression of the game. This scenario is detailed in Scenario 3: Social Media and Passwords.

Subsequently, the player must examine specific emails to determine whether they are potential phishing emails. The player can review and classify the emails as legitimate or phishing. Correctly identifying all emails as either legitimate or phishing allows the player to continue the game. However, making errors in classifying the emails necessitates replaying the episode. The episode concludes with a summary of the topics covered.

Episode 2 - The job

The second day, and consequently the second episode, commences with a relatively straightforward task for the player. The initial access code for the building has been altered, with the player provided a clue regarding Computer Security Day. After conducting a quick Google search, the player can deduce the date 3011 as the new access code.

Upon arriving at their workplace, the player receives multiple messages from colleagues introducing them to the concepts of phishing and vishing. The first email directs the player to a suspicious fake website, where they must identify three typical indicators of a fake website. This scenario is detailed in Scenario 2: CEO Fraud. Subsequently, upon identifying these markers, the player receives another message, detailed in Scenario 4: SMS/WhatsApp Phishing Scenario/Smishing - Identity Theft, instructing them to visit a colleague and vacate their workstation. The player must then adhere to the clean desk policy (take their ID and smartphone, shut down their computer) before departing the workplace.

The subsequent scene in this episode features a phone conversation between the employee and their "supervisor," during which vishing indicators are demonstrated, indicating a compromise in the bank's security. (Refer to Scenario 1: Identity Theft via Social Engineering (Vishing) and Phishing of Bank Data.) Following the conversation, the player receives a new phishing email attempt (which they can accept or reject). The subsequent tasks focus on social media awareness, requiring the player to uncover three crucial pieces of information from their supervisor's social media account to uncover clues regarding the supervisor's email account password.

Episode 3 - The Hacker

In the third episode, titled "The Hacker," a role reversal occurs for the player, transitioning to a "white hacker" narrative to gain insight into the attacker's perspective. The episode unfolds with the avatar receiving a message from the CEO of the ECS bank, acknowledging termination but expressing a desire to leverage expertise externally. In this capacity, the CEO tasks with testing the security of the bank's systems.

Accepting the assignment, the investigation begins. The initial objective is to delve into the Dark Web to gather information about the company. Successfully retrieving a list of company emails and employee phone numbers, these are used to orchestrate phishing and smishing campaigns. Concurrently, inspection on the employees' social media profiles identifies one individual who shares a significant amount of personal information. Leveraging this data, attempts are made to uncover their access password.

Subsequently, the avatar reconnects with the CEO of the ECS bank to relay findings regarding the company's Dark Web exposure and the susceptibility of accounts through campaigns and social media investigation. Additionally, recommendations for security protocols to fortify the bank's systems are provided. The CEO acknowledges the significance of appointing a Chief Security Officer (CSO) with comprehensive cyber security knowledge.

Refer to Scenario 5: White Hacker for further details on this scenario.

Episode 4 - The Expert

This serves as an additional bonus campaign for players in the form of a quiz. Here, players can test and refresh their knowledge of cyber security through a multiple-choice format. Each question presents four possible answers, with the correct choice accompanied by detailed explanations and additional information. A total of 40 different questions are included in this quiz. Refer to Scenario 6: Awareness Campaign for further details on this scenario.

The six scenarios, which form the basis for the aforementioned episodes, are elaborated upon below. These scenarios are directly aligned with the procedures and principles outlined for learning scenarios in Chapter 3.

5.2 Scenario 1: Identity theft via social engineering and phishing of data

Part 1 – Vishing-Voice Phishing

The individual receives a call from an unfamiliar number on their mobile phone. The caller, presenting themselves as a member of the victim's bank's security team, adopts a friendly manner and explains that they are reaching out due to recent phishing incidents reported by other customers. Allegedly, the bank's cybersecurity department is proactively calling customers to provide advance warning.

During the conversation, the caller demonstrates knowledge of the victim's full name and their status as a customer at the bank in question. They engage in friendly conversation while subtly probing the victim with security-related questions. By building up his competence in this way, he strengthens his position with the victim and gains more trust on the phone.

Towards the conclusion of the call, the caller predicts that the victim will likely receive a convincing phishing email purportedly from the bank. They advise the victim to watch for specific signs indicating it as a phishing attempt and emphasize the importance of promptly deleting such emails.

Additionally, the caller informs the victim that they will soon receive an email from them, complete with their full name, and requests the victim to enter their login credentials in the email. They claim that the bank's security department, where they purportedly work, intends to verify the integrity of the victim's bank account. Trusting the caller's assurances, the victim agrees to comply with the request.

Part 2 -The Phishing attack

The following day, as anticipated, the victim receives the phishing email from her bank. Armed with the information provided by the caller the day before, the victim easily spots the phishing indicators in the email. The sender's details are incorrect, the email lacks the correct address, and a contact person is absent from the signature. Additionally, the link provided in the email is suspiciously lengthy.

Recognizing the email as fraudulent, the victim promptly deletes it. As predicted, an hour later, the victim receives an email from the caller as promised. Everything unfolds exactly as foretold by the caller. Following the instructions in the email, the victim clicks on a link to enter her login credentials.

Upon clicking the link, the victim is directed to a website that appears to be the bank's official site. A special notice on the site emphasizes the need for enhanced security against future phishing attacks. To proceed with the security check, the victim is prompted to log in and authenticate herself to the bank by entering a username and password.

After submitting the login credentials and clicking the "Login" button, the victim receives a message stating that the entered data cannot be associated with a user account. Unrecognised to the victim, the entered data has been intercepted by the attacker as the victim was redirected to a fake website rather than the actual banking institution's site. The victim is seamlessly redirected to the legitimate banking site with the error message, minimizing suspicion.

Upon successfully logging in on the subsequent attempt, the absence of any security check against phishing or similar threats becomes apparent. Recognizing the attempted attack, the victim promptly changes the password, rendering the compromised data obsolete. The final password change is the solution to the first challenge!

Learning Objectives of this Scenario

By the end of this scenario, learners will be able to:

- recognize and classify selected vishing calls.
- recognize and classify selected phishing e-mails.
- understand and be aware whether the e-mail/call is from the company or not.
- recognize and understand the difference between real company’s website and a fake one.
- take care to manage and give personal bank details.
- understand basic principles of social engineering used by criminals.

What kind of various voice-phishing methods were used?

- The caller is friendly and attentive, addressing the victim by name.
- Introduces themselves with a full name and claims to hold a position of authority in a security team, fostering trust.
- States the purpose of the call is to protect the victim and ensure their safety.
- Demonstrates extensive knowledge about cybersecurity, enhancing their credibility and trustworthiness.
- Predicts the likelihood of a phishing email and advises the victim on where to identify potential signs of phishing.
- Poses as highly skilled individuals, known as Human Hackers, capable of quickly building trust over the phone.
- Calls often originate from unknown numbers or fake special divisions.
- Attempts to persuade the victim to take specific actions.

Learnings: How to protect yourself

Fake calls – Vishing:

- Never agree or do anything what the caller wants from you directly.
- Verify the caller's credibility by asking for details such as your personal bank consultant's name or the duration of your customer relationship.
- Immediately report the call to your bank by calling or visiting them.
- Conduct a search online to see if similar methods have been reported elsewhere.

Fake sender address: Be cautious of fake email addresses created by attackers, which may include letter swaps or substitutions with similar-looking characters.

Time pressure: Attackers often build up psychological pressure by asking the victim to take direct action. They try to tempt the victim to act rashly and hastily. Remember that urgent inquiries can usually be addressed directly by phone call, and do not necessarily require immediate action.

Uncertainty:

- Scrutinize phishing emails for spelling mistakes or inconsistencies.
- Question why a bank would request important documents via email when they could be securely transmitted through the bank's own Internet portal.

Implementation Notes:

- The "Story" should be presented in written text to inform participants about their role and the access data required.
- Open an email inbox with an unread message from a bank.
- Create a phishing email.
- Create and configure a fake banking website.

- Consider using GoPhish as an implementation tool.
- Develop and distribute handouts for participants via website, email, etc.

5.3 Scenario 2: CEO Fraud

Scenario Summary:

The player has recently been promoted and now holds a senior position. A few months after the promotion, he receives an e-mail from his CEO:

> *Dear Sir/Madam,*
>
> *Since your promotion, you have caught my attention with your outstanding performance. In just a few months, you have shown how valuable you are to our company and that you tackle problems quickly and in a goal-oriented manner. That is why I am writing to you now on this strictly confidential matter. Together with our partner law firm Meinhardt und Gerner, we are planning a merger of a chip manufacturer in China. This merger would give us a massive advantage over our competitors. Time and confidentiality are therefore the decisive factors in this merger.*
> *Dr. Gerner, my long-time friend and attorney, will call you shortly and discuss everything else with you. Under no circumstances should you talk to other colleagues about this merger. You, Dr. Gerner and I will work exclusively together on this. Communication between us will take place by e-mail and between you and Dr. Gerner by telephone.*
> *If we organize this merger quickly, you can look forward to a big bonus for Christmas.*
>
> *Yours sincerely*
> *CEO*

Shortly after, the phone rings, and Dr. Gerner from the law firm Meinhardt und Gerner introduces himself. He summarizes the email from the CEO and emphasizes the project's strict confidentiality. Dr. Gerner informs the player that they will receive an email with all the necessary details. To facilitate the merger, a deposit of €134,983 to the enterprise account is required, as they are acting as negotiators on behalf of the company. The player is instructed to arrange this payment, as they now have the authority to make such decisions following their recent promotion. Dr. Gerner concludes the conversation with a reminder of the importance of maintaining absolute confidentiality.

An hour later, the player receives an e-mail from his CEO:

Dear Sir/Madam
Dr. Gerner has already given me feedback concerning your recent phone call. You did a great job! All questions should be clarified. Wait for the e-mail from Dr. Gerner and then do everything exactly as he asks. I have already communicated the 134.983€ with the Board of Management and everything has been agreed so far.
Yours sincerely
CEO

10 minutes later, the player receives a top-priority email from Dr. Gerner:

Dear Sir/Madam
As just discussed with you on the phone. Please transfer immediately the deposit of 134.983€ to the following account:

DE 14 5005 6688 1189 0076 21
Intended purpose: Fusion China

If you have any further questions, please do not hesitate to call me on my mobile phone number.
With kind regards
Dr. Gerner

Now the player must choose between the following options:

1) The player complies with the request and "loses" the scenario. This is followed by an explanation regarding CEO Fraud.

2) The player refuses to transfer the money and instead informs their direct superior. The scam is exposed, and the player "wins" the scenario.

Learning Objectives of this scenario

After completion of this scenario, learners will be able to:

- recognize and classify fake e-mails by the company and/or company personnel.
- make sure each time to verify the real sender/recipient of the e-mail/call.
- take care to manage and give personal bank details.
- are beware of insistent and rapid requests for payment.

Users learn the basic principles of social engineering and especially the psychological mechanics of CEO fraud:

- Language used by social engineers.
- Human hacking basics.
- Knowledge of typical fraud e-mails (social engineering markers).

What type of social engineering / CEO fraud method was deployed?

The first email demonstrates the psychological tactics employed in CEO Fraud. Here are the key elements highlighted from the first email:

- The player is praised for their performance, being flattered with compliments.
- The player's highest-ranking superior contacts them directly and personally selects them for a task.
- The email demands absolute confidentiality and emphasizes the need for swift action.
- An unknown third party in a high position is introduced as the player's sole contact person.
- The contact person is portrayed as a friend of the CEO, implying that the player is now part of an exclusive inner circle.
- The email hints at a financial bonus as an incentive.

Dr. Gerner's Role:

- Dr. Gerner reinforces the CEO's email by providing insider knowledge, creating the illusion of genuine familiarity with the CEO.
- He subtly applies pressure to ensure a quick transfer of funds.
- Dr. Gerner presents himself as a trustworthy contact person, aiming to gain the player's confidence.
- He provides detailed instructions for the transaction.

Second Email from CEO:

- The second email provides reassurance by specifying the amount and stating that the board has approved the transaction.
- It includes further compliments and praise, reinforcing the positive image created in the initial email.
- A financial bonus is held out in prospect.

Learnings: How to protect yourself

- Never rely exclusively on email communication, especially for financial transactions.
- Exercise caution when dealing with strangers over the phone and question their intentions.
- As a first step, research the purported company or law firm online.
- Understand that mergers, acquisitions, and similar processes involve numerous individuals, not just a handful.
- Refrain from sharing confidential information over the phone or via email.

- Contact your immediate supervisor, CEO, IT department, or HR department directly and in person for verification.

Implementation Notes

- The implementation notes closely resemble those of the previous scenario.
- Story elements are customizable and adaptable.
- Incorporating a phone call with immediate in-game choices and varied outcomes would be beneficial if feasible.
- Ideally, the player should be given a brief window of time to make decisions (maximum 5 seconds).

5.4 Scenario 3: Social media and passwords

Scenario Summary

Part 1 – Innocent questions

In this specific escape room scenario, the objective for the user is twofold: to create secure passwords for their multiple accounts while also avoiding the pitfalls of social media posts that prompt unauthorized security questions for accounts.

During this scenario, the player engages online and actively navigates through various social networks. They interact with posts by commenting on them, rating them (e.g., with "likes"), engaging in dialogue with other users, and composing their own posts. If the user encounters various appealing posts on platforms like Facebook, they respond to them promptly. These may include humorous posts with titles such as:

“Do you remember your first car? What brand and model did you drive first?”

“The school time was very beautiful - to which elementary school did you go at that time? Maybe you will find old friends again!”

“First names now and in the past - Today the most popular first name is XYZ, back then it was ZZZ - what is your mother's / father's first name?”

“Nobody forgets his first pet - What was your first pet and what was its name?”

The user discovers numerous comments from individuals who share similar sentiments under the post. They all recall nostalgic experiences such as their first car, elementary school days, or their first pet.

These contributions are attractively presented, written in a friendly tone, and encourage the user to "participate." The user is prompted to respond to the questions posed in the scenario accordingly.

Part 2 – Dangerous questions

This section explains to the user the potential dangers associated with such posts. While they may appear harmless, these posts often leverage nostalgic sentiments to lower the user's caution while using internet applications.

In reality, however, such posts can be made by criminals seeking to obtain answers to classic security questions for accounts and passwords. Many accounts and websites utilize security questions as a means of password recovery or authentication in case users forget their passwords or input them incorrectly multiple times. Since many users use their real names on platforms like Facebook, criminals can obtain their first and last names along with answers to personal security questions.

Part 3 – Creating a Secure Password

The player now faces the scenario where their various accounts are potentially vulnerable to hacking. As a result, they are advised to create new, unique passwords for the five accounts in question. Up until now, their passwords have been simple and easy to remember, often using the same password for multiple accounts.

Passwords are Not Like Fruit

In the past, users were often advised to change their passwords regularly, leading them to create simple passwords for ease of memorization, making them susceptible to hacking.

In reality, passwords are not perishable like fruit and do not become insecure after a certain period. A strong and complex password remains secure over time.

To illustrate how quickly simple passwords can be compromised, here is a brief overview of typical passwords:

Password	Resistance to a brute force attack
12345678	Under one second
123123	Under one second
hallo	Under one second
Qwertz bzw. qwerty	Under one second
Smith bzw. Schmidt (second name)	Ca. 2 seconds
Password	Ca. 2 seconds

How are passwords hacked?

Hackers use so-called brute force attacks to crack passwords. These are lightning-fast automated entries that simply try out all possible combinations. With a number combination, this could look like this, for example:

100000

100001

100002 ... etc

Number combinations are particularly easy to hack due to the limited number of characters 0-9. Thereupon, entire dictionaries and other lists are often used by hackers.

A secure password

Basically, with passwords, anything that the keyboard allows can be used. It is important to remember the password well. When choosing a password, between two categories can be distinguished:

1. long string and not very complicated
2. shorter string and very complex

Long strings of characters are difficult for hackers to crack yet easy for users to remember. In this case, the password can consist of several words connected by underscores.

For instance, if our user, John, spent a semester abroad in Wroclaw in 2012, a secure password could be a combination of these elements: "John_study_Wroclaw_2012." This type of password would take several million years to crack, as the individual elements (John, study, Wroclaw, and 2012) could each be cracked in only a few minutes or seconds.

Alternatively, a shorter complex character string like "Xo55!mw$_08Lz" would also take several million years to be hacked with an ordinary PC. The user is now prompted to create a secure password and set it up for five accounts. If the player attempts to use the same new secure password for each account, an error message will appear.

Solution: Never use the same password across all your accounts. If a website or provider is hacked, hackers will gain immediate access to your password. Subsequently, they will test the combination of your email address and password on several other accounts. It's essential to use a different password for each account rather than relying on variations of a single password.

Learning Objectives of this scenario

After completing this scenario, learners will be able to

- understand the basic principles of social engineering on social media.
- carefully select personal information shared via social media.
- recognise "funny and harmless" posts on social media as a potential threat.
- understand how easy it is to hack a password.
- know how to create a safe password.

Social Media

Basic principles of social engineering in social media are recognised.

- Sensitisation to harmless-looking and funny postings is ensured.
- Caution with personal information in social media is recognised as necessary.

Passwords

- Basic knowledge about password security.
- Information regarding the durability of an insecure and secure password.
- Easiness of hacking a password.

Learnings: How to protect yourself

- To manage all passwords, it is recommended to use a password manager with a very strong master password.
- Use long string passwords which are easy to remember.
- Never place the passwords nearby own computer on a post-it notes or something similar.
- Users should not fall for funny or harmless post which asks peculiar questions like the ones mentioned before.

Additional Old-school advice: Use of a notebook in which all logins and passwords are entered. This book should be kept safely at home.

Implementation Notes

- If feasible, include a live demonstration showcasing how quickly a simple password, such as "password," can be cracked.
- Implement the "Clean Desk Policy" in the game, requiring the player to ensure their virtual desk is "clean" before they can proceed.
- Include a task where the player must create or use a password during the scenario.

5.5 Scenario 4: SMS / WhatsApp Phishing Scenario/ Smishing – Identity Theft

Scenario Summary

The player is on a business trip and receives a text message on his mobile phone:

> *Hello Sir/Madam*
> *my old cell phone broke down and I had the company give me a replacement. This is my new number: 0176/85935600. You can delete my old number directly and save the new number!*
> *Write me a WhatsApp so I can see if it worked, it's urgent!*
>
> *Thanks!*
> *Sincerely*
> *CEO*

The player doesn't mind, he deletes the old number and saves the new number. He then writes a WhatsApp message to the new number.

The answer comes directly:

> *Hello Sir/Madam*
> *My old phone has problems with the card, so I quickly got a replacement. I am currently on the road / in meetings and only available via WhatsApp. Do not call me.*

He answered. Shortly after that, another message comes directly:

> *I really have a huge problem on my mind right now. I need you to do this job for me urgently!*

He replies to it accordingly and a new message arrives:

> *I need to transfer two bills very urgently today and on my new cell phone I do not have my company bank details. Please transfer the sums immediately with your company credit card.*

He asks what kind of bills need to be paid and how much it is:

> *Invoices/payments for my hotel and dinner. That is 1.199 €. Do it today please. I will get back to you directly tomorrow morning.*

He agrees to pay.

> *Please pay it by real time bank transfer. Thus, we save on reminder fees. My assistant has once again forgotten to pay everything in advance.*

He becomes suspicious and writes that he is travelling and cannot undertake online banking at the moment.

Then just give me the number of your company credit card, expiration date and the security code, then I pay it directly and you don't have to do anything. I will then write you a receipt.

He replies that he will take care of it as soon as he gets home.

Okay great! I will not forget that you helped me discreetly!

He replies that he needs the bank details for the transfer and receives the answer immediately:

Hotel SuperInn
IBAN: DE29 0007 1236 5588 6758 22
Intended Use: Overnight Stay and Dinner
Sum: 1.199 €
However, it is better if you give me the credit card details, then I will do it from here.

What has happened?

Attackers have sent the victim a text message, expecting a reply. It's possible that the victim's phone number has been sold on the Darknet. Now, the attackers are attempting to deceive the victim into deleting their manager's old number under the guise of providing a new one. Urgently, the victim is asked for assistance in a pressing situation, often involving the payment of an invoice.

These requests typically involve small to medium amounts that appear innocent and fall within normal business expenses. The transfer is emphasized as urgent and must be completed in real-time, often citing reasons such as reminder fees or penalties. In some cases, credit card data may also be solicited as an alternative payment method. The criminals operate with a high level of organization, work similar to call centers, and employ this method to contact several numbers daily.

Learning Objectives of this scenario

After completion of this scenario, learners will be able to:

- recognize if a text messaging comes from a hacker (smishing)
- beware of insistent and rapid requests for payment
- beware of strange and unknown numbers
- take care to manage and share personal bank details

Learnings: How to protect yourself?

- Be alert! Any text message or call from an unfamiliar number should raise suspicion, especially if the person claims to be a supervisor or friend.
- Ask yourself: Why is the person using a different communication channel than usual?

- Avoid clicking on links in messages.
- Refrain from sharing important data such as credit card or PayPal information.
- Do not proceed with any form of money transfer.
- Reach out to co-workers, team members, or friends to verify the legitimacy of the SMS.
- Contact the specified person using their known, old number to confirm the information.
- Conduct an online search using the message content to check for warnings about similar messages.
- When in doubt, always reach out to your security department or the authorities/police.

Implementation Notes

- The theme can be used in different scenarios/ episodes - each with different outcomes.
- Players should be able to choose between different answers/actions.

5.6 Scenario 5: White hacker

Scenario Summary

In this scenario, the CSO from the first escape room (Episode 2) hires a so-called white hacker to conduct a penetration test in his company. The hacker's task is to execute a series of simulated cyber-attacks, including a phishing mail, a smishing attack, and attempts to crack common passwords, with the goal of infiltrating the system. Additionally, the hacker orders a social engineering call via the dark net to accompany the attack vectors.

By employing the same attack methods used in previous scenarios but from the perspective of a hacker, this scenario serves as a reverse engineering exercise to understand attack patterns. This allows users to gain insights into how different cyber security threats operate, empowering them to better protect themselves.

1. Phishing Email:

The hacker is tasked with creating a phishing email or assembling it using modular components. This involves selecting various text fragments and elements for the email:

- Sender details (email address, sender name)
- Main text with a compelling call to action to create urgency.
- Fake hyperlink to lure the recipient into clicking.
- Attachment containing ransomware.
- Signature

Afterward, the player checks off each component to ensure all elements of a phishing email are included. The function of each email element in a phishing attack is explained, and every correctly chosen component earns the user a point.

2. Smishing Attack:

The hacker conducts a live smishing attack on a selected target, choosing from three different targets (same as those in part three passwords) who will communicate with him via a messaging platform. The victims respond to his text messages.

The player selects from predefined text blocks and sends them "live" to the target. The target responds to each text block according to a predetermined function.

Example: Hacker sends text block A – target person replies with answer A, etc. The hacker should try to obtain sensitive information and/or manipulate the target person towards performing an unauthorised action.

Examples for texting:

White Hacker messages	Target answers	White Hacker second message
Hi, this is Justin from CorpSec – how are you? Right now, we are testing a new security direct chat tool for our bank. Did you get the e-mail?	Hi, no I did not get the email yet, what is this all about? Should I talk to my supervisors?	Oh, that should not be so. Perhaps you will get it in the next minutes. Anyway, we need to update your computer, to do so we will take a few steps together via this messenger.
Hello, my name is Mr. Boss, give me immediately all your passwords or I will fire you.	Nice try, I will block you.	End of game.
Hey, Martin is the Name of the guy from controlling? Are you sitting at your desk?	Err, yes, why are you asking?	I just got a weird message on my phone from CorpSec – Did you get it, too?
Here is the Hacker – do exactly as I say. Your system is compromised! If you do not do what I demand, it will cost you your job.	I call the IT department and the police.	End of game.

3. Passwords

The hacker has obtained information about the email address structure used in the company, which consists of firstname.name@bigbank.com. Targeting three individuals, the hacker has created profiles for each based on an OSINT (open-source intelligence) analysis.

1. Assistant to the CEO: Karen Maren

- Owner of a cat named Fluffypuffy, often shares cat pictures.
- Born on 12.06.1990, zodiac sign Gemini.
- Frequently engages in esoteric discussions on SM, follows a guru named SwingFlow.

Password suggestions: Cat, Fluffypuffy, Gemini, SwingFlow, (as well as some deliberately false suggestions)

2. Clerk: John Doe

- Enthusiast of his sports car nicknamed "The Duke" on internet forums.
- Passionate supporter of Manchester United, shares photos from matches.
- Holds sentimental value for his first car, known as White Fury.

Password suggestions: The Duke, musclecars, Manchester United, ManU, White Fury, (along with some intentionally false suggestions)

3. PR employee: Norbert Network

- Active across various social media platforms, frequently shares quotes from Henry Ford.
- Avid hobby cook and admirer of Gordon Ramsay.
- Film buff, especially fond of fantasy and Lord of the Rings.

Password suggestions: Henry Ford, Gordon Ramsay, Kitchen Nightmares, Lord of the Rings, LotR, Gandalf (and a selection of misleading suggestions)

Based on these profiles, the white hacker must select potential passwords. Each correct answer earns one point.

Social Engineering Joker: As a reward for completing a successful penetration test, the white hacker can request a social engineering attack on the darknet as a wildcard (keyword: cybercrime as a service) to expedite solving one of the three tasks.

The social engineering joker facilitates the following:

1. **Phishing**: A social engineering call accompanies the phishing email, ensuring immediate success by validating the phishing attempt.

2. **Smishing**: The target receives an email, paired with a smishing attack, urging a response via messenger.

Example: "Our security department is currently testing communication via Messenger - please cooperate immediately if you are contacted."

3. Password: A social engineer infiltrates the company to physically obtain passwords, as the targets have written them down on their desks.

Learning Objectives of this scenario

After completion of this scenario, learners will be able to:

- create a phishing e-mail with all the key components.
- replicate a smishing attack and its functioning.

* understand the process to find out a password.

- understand the mechanism and the danger to apply a social engineering attack.
- recognize that even the best hard- or software cannot protect anybody for 100%.

Learnings: How to protect yourself?

In the role of a "white hacker", the player is the attacker - albeit with good intentions. So, there is no need for protection. The key learning point here will be to change the perspective, so that players are able to see how all the mechanisms previously learnt apply to an attack scenario.

Implementation Notes

- The White-Hacker can try to attack the system.
- Reverse of the attack pattern has to be displayed - now the player has to obtain information e.g. from a social media profile to enter an account for example.

5.7 Scenario 6: Awareness Campaign

Scenario Summary

Story: Following the "success" in the initial escape room and the "excellent collaboration" with the white hacker, the Chief Security Officer (CSO) and the white hacker gain increasing recognition in the security world. However, their prominence attracts the jealousy of the Chief Evil Officer of an exceptionally evil bank. Consequently, the CSO and the White Hacker are summoned to this evil bank and are forbidden to leave until they devise the ultimate awareness concept.

Preface: In this scenario, the player's task is not to learn new cyber security principles or attack methods. Instead, they are tasked with creating an awareness campaign about cyber security. Particularly for small and medium-sized enterprises (SMEs) lacking resources to engage a service provider for such campaigns, it is crucial that they learn to create them independently with the resources available.

1. Get to Know the Status Quo Inside the Company:

The player must ascertain the current state of awareness training within the company and assess the knowledge level at the evil bank. The player has several options to obtain this information, with the correct answer highlighted in bold. Upon selecting the correct answer, the player receives an explanation.

- Randomly ask coworkers about their knowledge of cyber security.
- Send an email to all employees requesting a summary of their knowledge about cyber security and training.
- **Initiate a Head Start meeting with the CEO to discuss the new cyber security strategy, followed by creating a digital questionnaire about cyber security, training, and awareness, to be completed anonymously within two weeks.**
- Hire an expensive service provider with sufficient funds and delegate the task to them.

2. First Steps:

After determining the current situation within the company through a survey, the player proceeds to take the initial steps of the new awareness campaign. The objective is to establish a secure and alert company. The player selects the appropriate first steps, with the correct answer highlighted in bold, followed by an explanation.

- Order merchandise and informational materials from various providers about Cyber Security.
- Outsource the task to interns, as there is insufficient time during regular business hours.
- Hire a white hacker and social engineer for a penetration test to demonstrate vulnerabilities.
- **Develop a roadmap with different milestones and evaluation points to guide the campaign's progression over time.**
- Purchase e-learning and online training modules.
- Collect free whitepapers and YouTube videos for training purposes to save costs.

3. Creating an Awareness Campaign – Phishing:

The player's task is to devise a creative awareness campaign addressing the phishing issue. The chosen medium is A2 format framed posters, to be displayed throughout the company premises. The player selects text blocks for the posters via drag and drop.

The first poster will focus on handling emails from unknown senders, with examples of possible responses provided. The correct response is not initially disclosed to the player in the first escape room and the "great collaboration" with the white hacker, the CSO and the white hacker become increasingly well-known in the security world.

Right answers	Wrong answers
Check the address – do you know it?	Click on the link and attachment – time is money.
Did they ask you to do something or provide sensible data?	It is alright, nobody is going to hack a SME.
Do not click on a link or attachment.	The mail is from amazon, it sure won't do any harm…
If not sure – ask IT for help.	
Check the signature – is there an address or phone number you know?	

4. Creating an awareness campaign – the secure password

Secure passwords and awareness of information security are essential for every company. The player recognizes the significance of secure passwords and integrates this topic directly into the onboarding process. Each employee receives a comprehensive handout detailing how to create secure passwords and what criteria constitute secure passwords. Since having this information readily available for daily use is crucial, the player decides to have mouse pads printed with key tips and rules for password management. Encouraging employees to use these mouse pads daily reinforces awareness and reinforces best practices.

What information should be printed on the mouse pad, especially when space is limited?

The player must select between correct and incorrect answers; each correct answer earns one point.

Right answers	Wrong answers
Secure passwords consist of numbers, letters and special characters or long word strings.	Change your passwords on a monthly basis.
A good password is not a fruit, it won't get bad, you do not have to change it every month.	If you have a secure password, use it for every other account as well.
Use passwords that you can remember well but are not easy to guess.	Use passwords which are directly linked to you, like your dogs name, your favourite football club, etc.
Don't use just numbers, they are easier to hack than you think.	A long string of numbers like phone number is always good.
	Keep your password somewhere at your desk (under the keyboard) for emergencies.

5. Creating an awareness campaign – Smishing

Smishing is an emerging cyber-attack that combines elements of phishing and social engineering. What sets it apart is the interactive communication via instant messenger, which is both anonymous and intimately close to the victim. This direct response nature makes the attack more engaging and potentially deceptive.

To incorporate the topic of smishing into the awareness campaign, the player must select from a variety of text fragments and respond appropriately to the victim's messages.

Example: The player sees a dialogue but at first only the victims' answers – so he has to choose the right text block according to the given answers.

Blank (choose answers from pool of text blocks)
Answer victim: Hi, yes this is Jessica from the front desk – do I know you.
Blank (choose answers from pool of text blocks)
Hm, I do not know----maybe I will talk to my superior first.
Blank (choose answers from pool of text blocks)
Okay that seems legit, what shall I do next?

Each correct answer earns one point. This game could be integrated into regular training sessions within a company to enhance awareness of smishing and social engineering attacks. It can be easily implemented using PowerPoint as a tool. For instance, each correct or incorrect answer could trigger a pop-up with detailed information and explanations. Gamification in awareness campaigns is a widely used technique that adds an enjoyable aspect to learning.

6. Creating an Awareness Campaign - CEO Fraud and Social Engineering - Final

Social engineering and CEO Fraud are closely linked, employing psychological manipulation to achieve their objectives. Therefore, establishing a successful campaign requires adequate knowledge. Fortunately, our CSO and the White Hacker have been collaborating and are now on the verge of escaping the evil bank escape room. Their objective is to persuade the evil CEO to release them by demonstrating that they have completed the awareness campaign. They must select from various dialogue options to convince the evil CEO and ultimately escape from the room.

Learning Objectives of this scenario

After the completion of this scenario, learners will be able to:

- understand how to create an awareness campaign about cybersecurity, especially for SMEs.
- understand which steps have to be taken to implement an awareness campaign and how to improve each step of it to enhance promotional achievements.

* understand how to create a safe and vigilant company on cybersecurity.
- understand how to implement an awareness-raising campaign about phishing.
- recognize and handle phishing emails.
- be aware of the modalities for dealing with passwords (creation and secure management).

Learnings: How to protect yourself?

Since the objective is to develop an awareness campaign, there is no need for protection measures. However, it's possible to outline the most crucial tips for creating such a campaign within a company.

Implementation Notes

The task of "creating an awareness campaign" could be executed in several ways:

- As a creative assignment (as detailed previously).
- Or as a downloadable summary or whitepaper focusing on the topic (e.g., the first five awareness tips).
- Or as a series of questions.

The outlined scenarios serve as foundational material for the levels or stages within the EyesOnCS escape room game scenarios. Beginning with "Scenario 1: Identity Theft via Social Engineering (Vishing) and Phishing of Bank Data," these learning scenarios align with the methods and principles outlined in Chapter 3, "Learning Scenarios." They are adaptable for integration into the actual development of the EyesOnCS game and for incorporation into the escape room game scenarios.

The scenarios outlined above exemplify various and common cyberattack vectors, accompanied by practical tips and solutions for real-world application. These game scenarios, detailed in the preceding chapter, are woven into four distinct EyesOnCS episodes. Upon successful completion of the escape room game as part of vocational corporate training, participants will develop a heightened awareness of the everyday dangers present in cyberspace. This enhanced awareness equips them to safeguard themselves and their companies more effectively.

6 References

Albrecht, S., & Revermann, C. (2016). Digitale Medien in der Bildung. Endbericht zum TA-Projekt (Arbeitsbericht Nummer 171). Büro für Technikfolgen und Abschätzung beim deutschen Bundestag (TAB).

Becker, W., & Metz, M. (2022). Digitale Lernwelten – Serious Games und Gamification: Didaktik, Anwendungen und Erfahrungen in der Beruflichen Bildung. Springer VS.

Bernardes, O., Amorim, V., & Moreira, A. C. (2022). Handbook of Research on Gamification Dynamics and User Experience Design. IGI Global.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. & Krathwohl, D. R. (1956). Taxonomy of Educational Objectives. The Classification of Educational Goals, Handbook I: Cognitive Domain. David McKay Company, Inc.

Caponetto, I., Earp, J., & Ott, M. (2014). Gamification and education: A literature review. European Conference on Games Based Learning, 1, 50.

Coughlin, V., Ho, M. R., & Alvarez, G. (2023). Escape the Room! Utilizing Gamification in a Preceptor Training Workshop. Journal for Nurses in Professional Development. https://doi.org/10.1097/NND.0000000000000977

EyesOnCS-Team.(2022), Compendium of Cyber Security Needs.(IO1), EyesOnCS

EyesOnCS-Team.(2023), The Implementation of the EyesOnCS Escape Room Game (IO3). EyesOnCS.
Friedrich, C., Teaford, H., Taubenheim, A., & Sick, B. (2020). Interprofessional Health Care Escape Room for Advanced Learners. The Journal of Nursing Education, 59(1), 46–50.

Gajanova, L., Nadanyova, N., & Majerov, J. (n.d.). Gamification as a Tool for Improving the Didactic Process. International Conference on Education, E-learning and Social Science (EELSS 2020)}.

Goertz, L., Fehling, C., & Hagenhofer, T. (2021). COPLAR-LEITFADEN, Didaktische Konzepte identifizieren –Community of Practice zum Lernen mit AR und VR.

Guckian, J., Sridhar, A., & Meggitt, S. J. (2020). Exploring the perspectives of dermatology undergraduates with an escape room game. Clinical and Experimental Dermatology, 45(2), 153–158.

Hammer, J., & Black, J. (2009). Games and (Preparation for Future) Learning. Educational Technology Research and Development: ETR & D, 49, 29–34.

Janssens, O., Samyny, K., Van de Walle, R., & Van Hoecke, S. (2014). Educational virtual game scenario generation for serious games. 2014 IEEE 3nd International Conference on Serious Games and Applications for Health (SeGAH), 1–8.

López-Pernas, S., Gordillo, A., Barra, E., & Quemada, J. (2019). Examining the Use of an Educational Escape Room for Teaching Programming in a Higher Education Setting. IEEE Access, 7, 31723–31737.

Maha, K., Jamal, B., Mohamed, E., & Mohamed, K. (2020). The educational scenario architecture of a learning situation. Global Journal of Engineering and Technology Advances, 3(1), 027–040.

Marczewski, A. (2015). Monkeys Like to Play: Gamification, Game Thinking &Motivational Design, CreateSpace Independent Publishing Platform. CreateSpace Independent Publishing Platform.

Mayer, R. E. (2019). Computer Games in Education. Annual Review of Psychology, 70, 531–549.

Mijal, M., Cieśla, M., & Gromadzka, M. (2020). Escape room as an adult education tool. Homo Ludens, 1 (13), 163–178.

Mugambi, P. (2021). The concepts of didactics and pedagogy,. Quora. https://www.quora.com/What-is-the-concept-of-didactic-and-pedagogy

Wikipedia.,Definition of PEDAGOG, https://www.merriam-webster.com/dictionary/pedagogy. WIKIPEDIA. Retrieved October 23, 2023, from https://www.merriam-webster.com/dictionary/pedagogy

Nationale Agentur. (2021). Enhancing Cyber Security - Development of trainings using "Escape Room" Model. DE02 - Nationale Agentur Bildung für Europa beim Bundesinstitut für Berufsbildung.

Wikipedia, Storyline-Methode. WIKIPEDIA. https://de.wikipedia.org/wiki/Storyline-Methode

Owa, M. (2022, November 30). What is Pedagogy: Definition, Principles & Application.

Plessis, E. (2011). Jak zákazník vnímá značku. Computer Press.

Praxis-Ratgeber für Bildungsinstitute: Lernspiele in der Erwachsenenbildung. (2021a). Bäretswil.

Prensky, M. (2005). Computer games and learning: Digital game-based learning. Handbook of Computer Game Studies, 18(2005), 97–122.

Rachels, J. R., & Rockinson-Szapkiw, A. J. (2017). The effects of a mobile gamification app on elementary students Spanish achievement and self-efficacy. Computer Assisted Language Learning, 31, 72–89.

Richter, K., & Müller, L. (2023, April). Berufliche Weiterbildung im Kontext der digitalen Transformation. Digitale Methoden und Medienformate zur Gestaltung beruflicher Bildungsinhalte.

f-bb-online 04/23. F-Bb-Online. https://www.f-bb.de/unsere-arbeit/publikationen/digitalisierung-in-der-grundbildung-didaktische-empfehlungen-fuer-einen-gelingenden-unterricht/

Roebers, F., & Leisenberg, M. (2010). WEB 2.0 im Unternehmen: Theorie & Praxis - Ein Kursbuch für Führungskräfte. Tredition Gmbh.

R. Rawassizadeh, C. Dobbins, E. Momeni, P. Mirza-Babaei, R. Rahnamoun. (2015). Lesson Learnedfrom Collecting Quantified Self Information via Mobile and Wearable Devices, Journal of Sensor and Actuator Networks, 4, 315–335.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. Future Internet, 11(4), 89.

Salen, K., & Zimmerman, E. (2003). Rules of play: game design fundamentals. MIT Press.

Squire, K. (2011). Video games and learning: teaching and participatory culture in the digital age. Teachers College Press.

Streim, A., & Mann, S. (2021). Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr. Bitcom. https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Tercanli, H., Martina, R., Ferreira Dias, M., Wakkee, I., Reuter, J., Amorim, M., Madaleno, M., Magueta, D., Vieira, E., Veloso, C., & Others. (2021). Educational escape rooms in practice: research, experiences, and recommendations. https://digibug.ugr.es/handle/10481/71565

Warby, N. (2023, October 11). Biggest AAA games coming in 2023: Avatar, The Finals, more. Charlie Intel. https://www.charlieintel.com/games/biggest-aaa-video-games-coming-in-2023-196534/

Werbach, K., & Hunter, D. (2020). For the Win-The Power of Gamification and Game Thinking in Business, Education, Government, and Social Impact. Wharton School Press.

Wössner, S. (n.d.). Gamification und Game-Based Learning: Eine Begriffsdefinition. Lmz Bw. Retrieved February 11, 2023, from https://www.lmz-bw.de/medienbildung/themen-von-f-bis-z/game-based-learning/gamification-und-game-based-learning-eine-begriffsdefinition

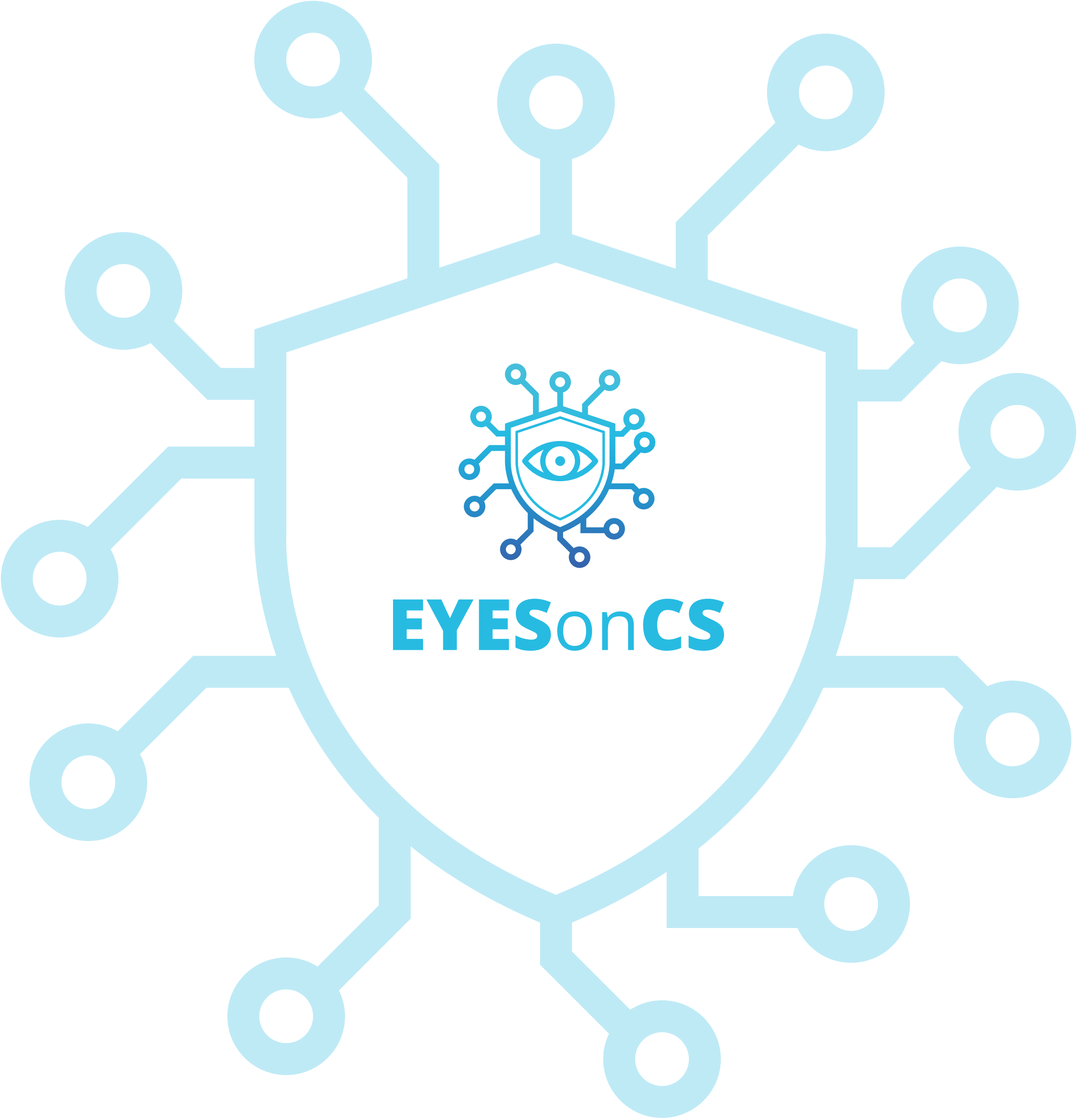
Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. & Krathwohl, D. R. (Eds.). (1956). Taxonomy of Educational Objectives. The Classification of Educational Goals, Handbook I: Cognitive Domain. New York: David McKay Company, Inc.

Brady, S. C., & Andersen, E. C. (2019). An escape-room inspired game for genetics review. Journal of Biological Education, 1–12, https://doi.org/10.1080/00219266.2019.1703784

Eukel, H. N., Frenzel, J., Frazier, K., & Miller, M. (2020). Unlocking Student Engagement: Creation, Adaptation, and Application of an Educational Escape Room Across Three Pharmacy Campuses. Simulation & Gaming, 51(2), 167–179. https://doi.org/10.1177/1046878119898509

Wikipedia., Didactic method. WIKIPEDIA. Retrieved November 28, 2023, https://en.wikipedia.org/wiki/Didactic_method

Notes



Stay tuned!

Follow us and learn more
about the project here:

www.eyesoncs.eu

Co-funded by
the European Union