Co-funded by the European Union

Digital Literate in VET by Cybersecurity Training with Immersive Technologies

CybARverse

CybARverse qualification model

Document prepared by:

Fundatia EOS – Educating for an Open Society with the contribution of SCP, LIA, CCS and Tech.mt project partners

March-23

Co-funded by the European Union

CYBARVERSE

PROJECT SUMMARY

CybARverse is an Erasmus+ co-funded project which supports IT as well as non-IT teachers and trainers' digital skills development, through the use of immersive technologies. The focus of this project is to train the target group on how to recognise and react correctly to cyberattacks. It promotes cyber security awareness, the implementation of the Digital Education Action Plan (Actions 5 and 7) as well as national agendas, and contributes to a more digital, greener and more inclusive teaching and learning.

Project no: 2022-1-LT01-KA220-VET-000089116

Objectives:

- To promote professional, personal, and digital skills among VET teachers and trainers in the field of cybersecurity.
- To incorporate modern and immersive technologies into VET cybersecurity training.
- Structured qualification of teachers and trainers to become cybersecurity aware and literate.
- To ensure the sustainability of the project results.

Project implemented by:

LANGAS | ATEITI

SCP School of Certified Professionals

CYPRUS COMPUTER SOCIETY

Tech.mt MALTA - LEADING THROUGH INNOVATION

eos FUNDAȚIA EOS ROMÂNIA

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission nor National Agency cannot be held responsible for any use which may be made of the information contained therein.

TABLE OF CONTENTS

1 INTRODUCTION 6

2 METHODOLOGY 7

2.1 Needs assessment 7

2.2 Educational Frameworks 7

2.3 Analyse industry trends and requirements for cybersecurity skills 9

2.4 Conduct a survey or group discussion with learners, instructors and industry professionals to identify gaps in existing cybersecurity education 9

2.5 Development of learning objectives 16

3 LEARNING MATRICES 18

3.1 A1 / Social engineering 21

3.2 A1 / Phishing 22

3.3 A1 / Social media 23

3.4 A1 / Grooming 24

3.5 A2 / Malware 25

3.6 A2 / IoT (Internet of Things) beginners 26

3.7 A2 / Pharming 27

3.8 A2 / Rootkit 28

3.9 A2 / Ransomware 29

3.10 B1 / SQL injection 30

3.11 B1 / Cross-Site Scripting (XSS) 31

3.12 B1 / Cryptojacking 32

3.13 B2 / DoS (Denial of Service) attack 33

3.14 B2 / DDoS (Distributed Denial of Service) 34

3.15 B2 / A zero-day exploit 35

3.16 B2 / IoT (Internet of Things) advanced 36

3.17 B2 / Man-in-the-middle (MITM) 37

4 Bibliography 39

LIST OF TABLES

Table 1: Social engineering Matrix 21
Table 2: Phishing Matrix 22
Table 3: Social media threats Matrix 23
Table 4: Grooming Matrix 24
Table 5: Malware Matrix 25
Table 6: IoT attacks Matrix 26
Table 7: Pharming Attack Matrix 27
Table 8: Rootkit Matrix 28
Table 9: Ransomware Matrix 29
Table 10: SQL Injection Matrix 30
Table 11: Cross-Site Scripting (XSS) Matrix 31
Table 12: Cryptojacking Matrix 32
Table 13: DOS Attack Matrix 33
Table 14: DDoS Attack Matrix 34
Table 15: Zero-Day Exploits Matrix 35
Table 16: IoT attacks Matrix 36
Table 17: Man-in-the-Middle Attacks Matrix 37

LIST OF FIGURES

Figure 1 - My organization's level 10
Figure 2 - How important do you consider Cyber Security awareness for? 10
Figure 3 - How would you rate personal level of awareness on cyber security issues? 11
Figure 4 - Role in the education sector 11
Figure 5 - Have you ever participated in cyber security trainings? 11
Figure 6 - What topics relating to cyber security do you consider important to know and be able to explain and support your students? (security at home, use of public wi-fi, working remotely, phishing) 12
Figure 7 - What topics relating to cyber security do you consider important to know and be able to explain and support your students? (use of email, malware, use of passwords) 12
Figure 8 - What topics relating to cyber security do you consider important to know and be able to explain and support your students? (security on social networks, social engineering, removable media security, mobile device security) 13
Figure 9 - What topics relating to cyber security do you consider important to know and be able to explain and support your students (man in the middle attacks, cloud security, internet safety, physical security) 13
Figure 10 - What topics relating to cyber security do you consider important to know and be able to explain and support your students (ransomware attacks, DOS attacks, cryptojacking attacks) 14
Figure 11 - What topics relating to cyber security do you consider important to know and be able to explain and support your students (IoT - internet of things attacks, SQL injection) 14
Figure 12 - How familiar are you with the use of Virtual Reality (VR) equipment? 15
Figure 13 - How familiar are you with the use of Augmented Reality (AR) equipment? 15
Figure 14 - Do you think that the use of VR/AR as an educational tool can be useful? 15
Figure 15 - would you be interested in participating in training sessions related to Cyber Security that will use VR/AR as a training tool? 16
Figure 16 - How would you use new media such as AR/VR for your own training and in your class? 16
Figure 17 - Cybersecurity levels (Cybersecurity awareness/ Cybersecurity expertise) 20

1 INTRODUCTION

The CybARverse qualification model for VET teachers and trainers is a public document whose purpose is to capture and describe the required competences for using immersive technologies (AR, VR/WEBVR) in cybersecurity training for a classroom environment. The CybARverse qualification model for immersive training, bases on existing training materials & forms and ensures a tailor-made and a pedagogical-sound use of teaching and training scenarios. This results in pedagogical transformation and relates to the urgent need to improve teaching personal digital literacy and therefore the safe use of digital technologies. The focus is on non-IT professionals and IT professions.

Impressive advances in information technology, particularly in robotics, artificial intelligence, bioengineering, genetic modification and similar fields, are having a direct impact on future occupations, which are becoming increasingly difficult to predict. Robotization, automation, artificial intelligence and virtual reality are already present, and forecasts show a significant increase in them in the economy of the coming years. In this situation, significant changes are taking shape in the labour market, which makes education systems anticipate the needs of the future, not just react to technological developments.

Creativity, entrepreneurial and managerial skills and responsible use of technologies will become constants of education in the twenty-first century. The digitalisation and rapid development of information technology, as well as the increasing and easier access to digital technology, are fundamentally changing both everyday life and patterns of networking between people and the characteristics of the labour market. The huge and constantly growing volume of information, as well as the spectacular development of the means that allow easy access to information lead to the spectacular advance of social networks. People and organisations are constantly becoming consumers and creators of media, and the level of interconnectedness generates behavioural patterns that were hard to imagine a short time ago.

2 METHODOLOGY

2.1 Needs assessment

The review of the curriculum and learning resources in the field of cybersecurity is an important step in the development of effective educational programs in this field. By examining what has already been developed, trainers can identify best practices and improvements that can be made and ensure that their own curriculum aligns with industry standards and current trends in cybersecurity integrated with modern methodologies.

The curriculum and learning resources in the field of cybersecurity need to include:

- Relevance: The curriculum and resources must be up-to-date and relevant to current cybersecurity threats and trends. Outdated information can lead to gaps in knowledge and leave educators unprepared to address emerging threats.
- Depth and scale: The curriculum must provide a comprehensive understanding of cybersecurity concepts, including technical aspects.
- Interactivity: Cybersecurity is a practical field, so it is important to incorporate interactive and practical activities into the curriculum. These may include simulations, practical exercises and real-world case studies using modern AR and VR technologies.
- Commitment: The curriculum must be engaging and attract the interest of VET educators. This can be achieved through the use of multimedia resources, interactive exercises and real-world examples.
- Assessment: The curriculum must include methods for assessing educators' learning and progress. These may include questionnaires, exams and practical assessments.
- Collaboration: Cybersecurity involves teamwork, so the curriculum should include opportunities for collaborative learning and teamwork.
- Accessibility: The curriculum and resources must be accessible to a diverse range of educators, including those with disabilities or from non-technical backgrounds.

2.2 Educational Frameworks

DIGICOMPEDU is a project launched by the European Commission in 2020, which aims to develop digital competences in education by providing educational guidelines and tools for teachers, trainers and educational leaders. DIGICOMPEDU envisages the development of both educators' and teachers' digital competences by providing innovative educational resources and tools tailored to the specific needs of each Member State of the European Union. The ultimate goal of the project is to contribute to the development of an inclusive and innovative digital society, able to face the challenges and opportunities offered by the ongoing digital revolution.

SAMR is a pedagogical model that encourages the use of technology in learning, and represents the acronym for Substitution, Augmentation, Modification and Redefinition, which are the four levels of use of technology in learning.

- Substitution: the use of technology instead of another similar tool or process without making significant improvements in the learning process. For example, using an electronic document instead of a printed document.
- Augmentation: The use of technology to add functionality and improvements to the learning process. For example, using document editing software to add multimedia elements such as images and videos.
- Modification: The use of technology to enable learning processes that were not possible before the introduction of technology. For example, the use of an online forum to allow discussions between educators from different countries.
- Redefinition: the use of technology to create entirely new learning processes that could not have been achieved before the introduction of technology. For example, using virtual reality software to create interactive and immersive learning experiences.

SAMR is a useful tool for teachers and trainers who want to integrate technology into the learning process and improve the learning experience of educators or learners. By understanding these levels, teachers can plan and implement learning activities that integrate technology in an efficient and effective way.

TPACK is the acronym for Technology, Pedagogy and Content Knowledge. It is a conceptual framework developed to describe the digital competences needed for the successful integration of technology into the teaching-learning process. TPACK argues that effective learning with technology depends on three types of knowledge: knowledge of the content of the disciplines, pedagogical knowledge and knowledge of technology. In order to successfully integrate technology into the teaching-learning process, teachers must have a deep understanding of each of these three areas and integrate them properly.

Knowledge of content refers to understanding the content of the subjects they teach, pedagogical knowledge is about understanding how educators learn, and knowledge about technology refers to understanding how technology can be used to support the teaching-learning process.

Specifically, TPACK highlights the importance of integrating the technology properly so that it supports both content and pedagogy. For example, learning through an interactive game can be an effective way to encourage learning through experimentation while improving the understanding of cybersecurity concepts.

TPACK can be applied in various learning contexts, including VET learning, to help teachers successfully integrate technology into the teaching-learning process and to support the development of educators' digital skills.

2.3 Analyse industry trends and requirements for cybersecurity skills

The industry has become increasingly dependent on information technology, making cybersecurity a major concern for organisations. Currently, skills in cybersecurity are essential for any company or organisation that uses information technology.

Here are some current trends and requirements for cybersecurity skills:

a) Strong technical skills: Technical skills are essential in the field of cybersecurity. These include knowledge of cryptography, computer networks, the architecture of security systems, and the ability to quickly analyse and respond to cyberattacks.
b) Knowledge of laws and regulations: With growing concerns about the protection of personal data and other sensitive information, governments have imposed strict data protection regulations. Therefore, competences in terms of compliance with cybersecurity laws and regulations are particularly important.
c) Effective communication: During a cybersecurity crisis, communication is essential. That's why communication skills are vital for a cybersecurity professional to be able to communicate clearly and effectively with colleagues, clients and other stakeholders.
d) Analysis and problem-solving skills: As cyber threats are constantly evolving, cybersecurity professionals must have strong analysis and problem-solving skills to be able to identify and address threats effectively.
e) Understanding cybersecurity risks for businesses: We've all heard about cyberattacks on large companies that have impacted their business and reputation. Understanding cybersecurity risks for business is vital for a professional in the field to be able to help the organisation take the necessary protective measures.
f) Innovation and adaptability: Cyber threats are changing rapidly, and cybersecurity professionals need to be innovative and tailored to stay abreast of the evolution of technology and be able to respond effectively to emerging threats.

2.4 Conduct a survey or group discussion with learners, instructors and industry professionals to identify gaps in existing cybersecurity education

Following the application of the survey to 77 teachers and trainers from LT, CY, RO and MT, the following conclusions were drawn:

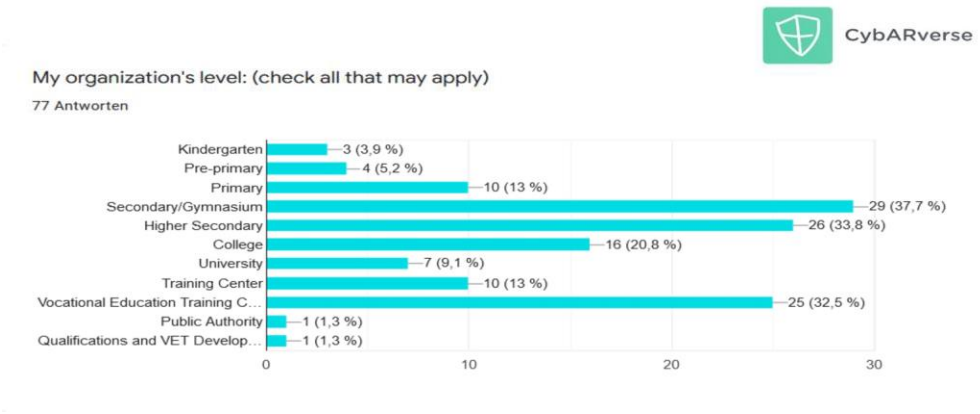


Figure 1 - My organization's level

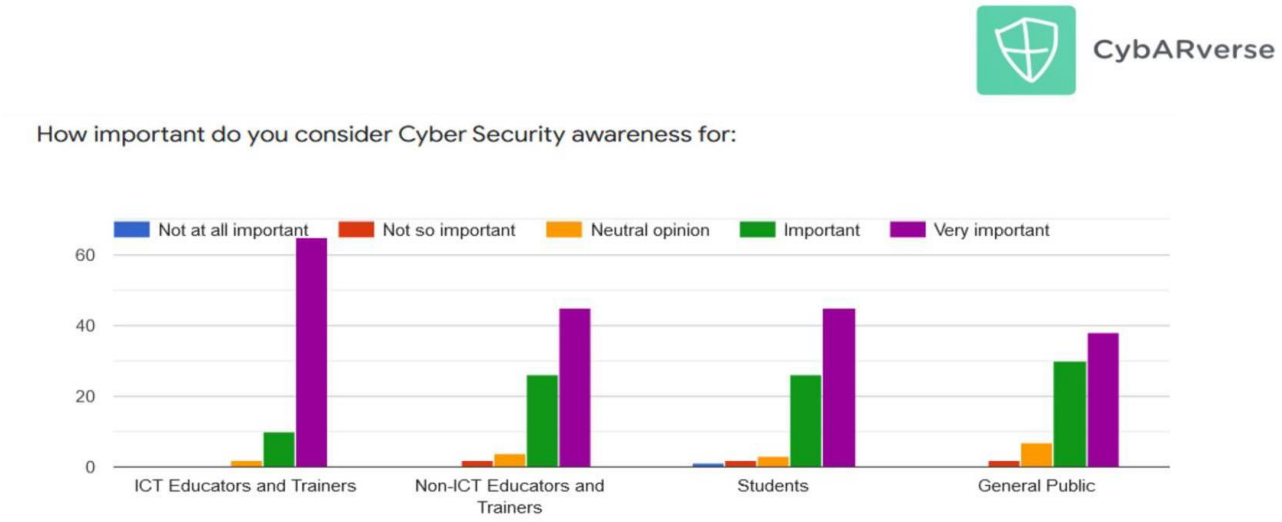
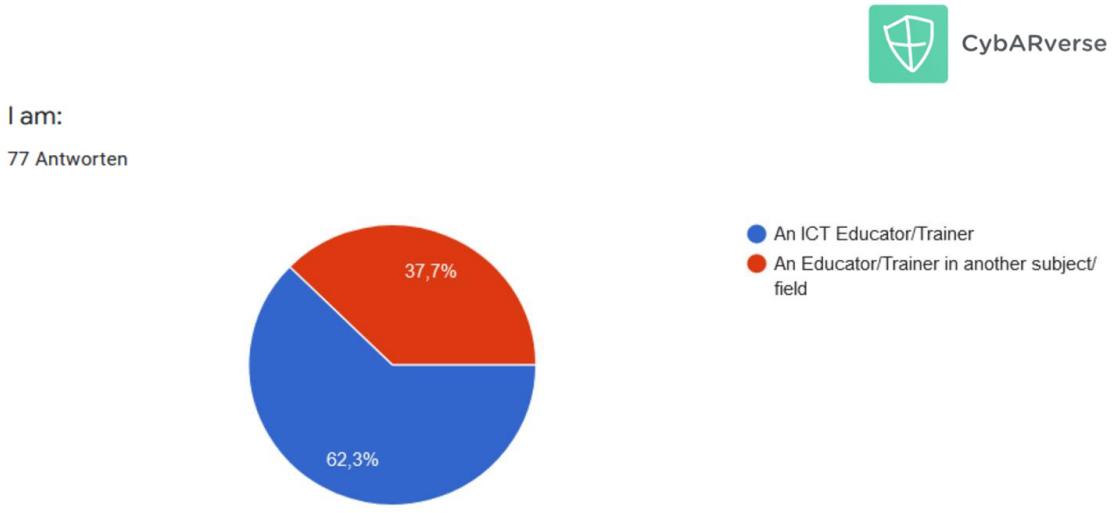


Figure 2 - How important do you consider Cyber Security awareness for?



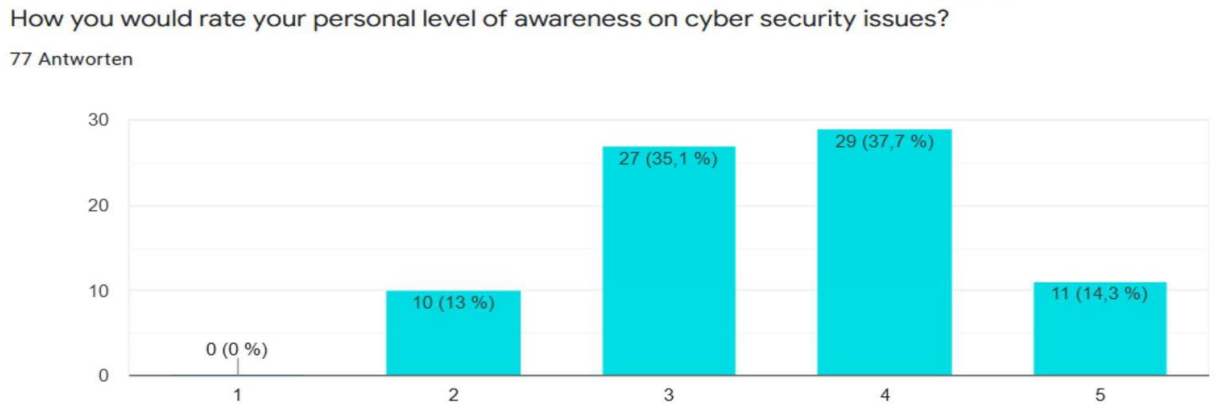


Figure 3 - How would you rate personal level of awareness on cyber security issues?

Figure 4 - Role in the education sector

CybARverse

Figure 5 - Have you ever participated in cyber security trainings?

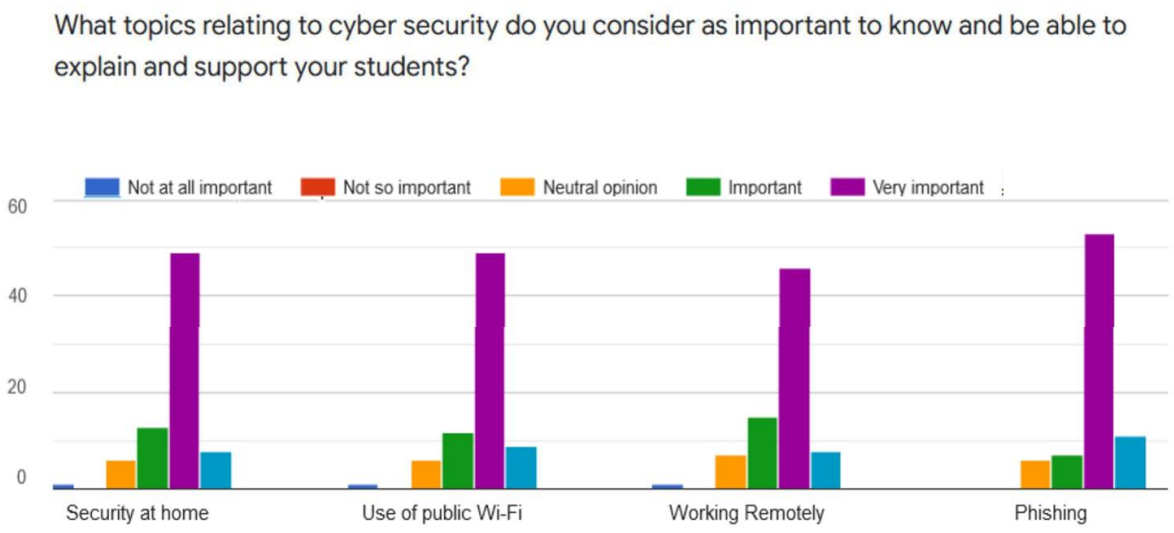


Figure 6 - What topics relating to cyber security do you consider important to know and be able to explain and support your students? (security at home, use of public wi-fi, working remotely, phishing)

CybARverse

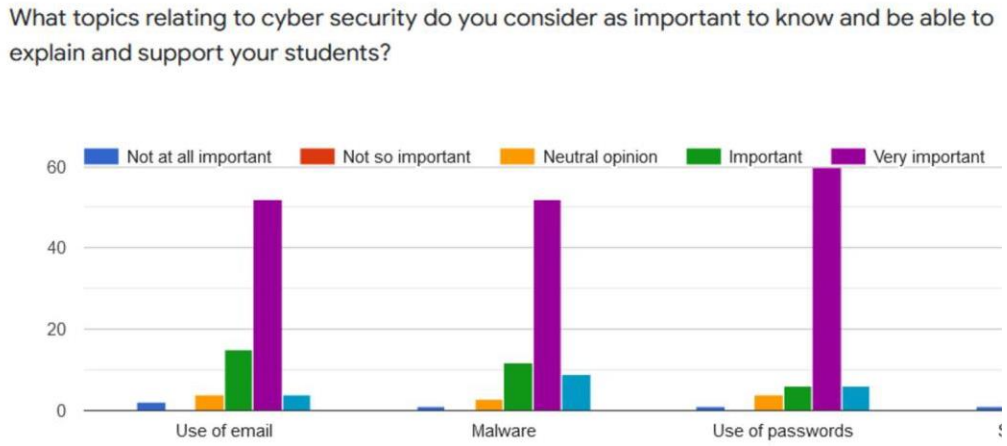


Figure 7 - What topics relating to cyber security do you consider important to know and be able to explain and support your students? (use of email, malware, use of passwords)

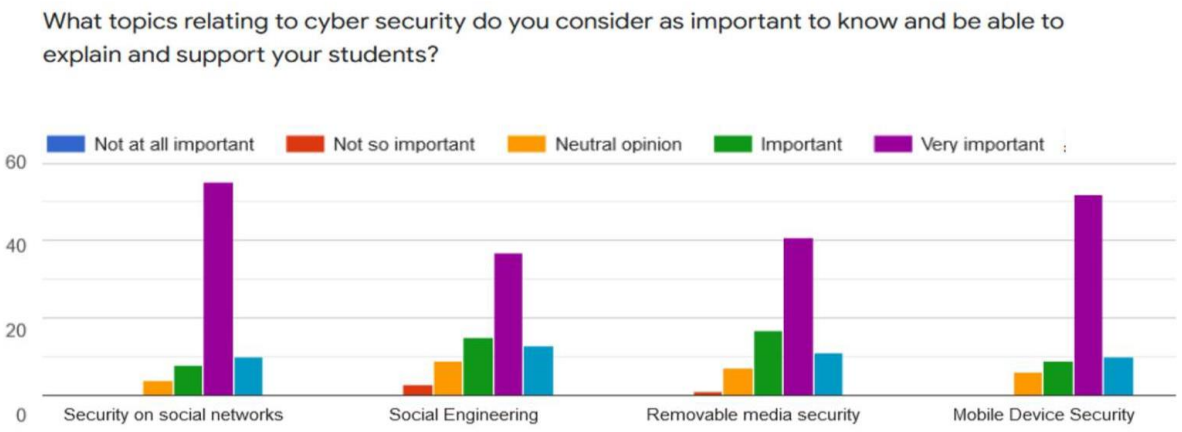


Figure 8 - What topics relating to cyber security do you consider important to know and be able to explain and support your students? (security on social networks, social engineering, removable media security, mobile device security)

CybARverse

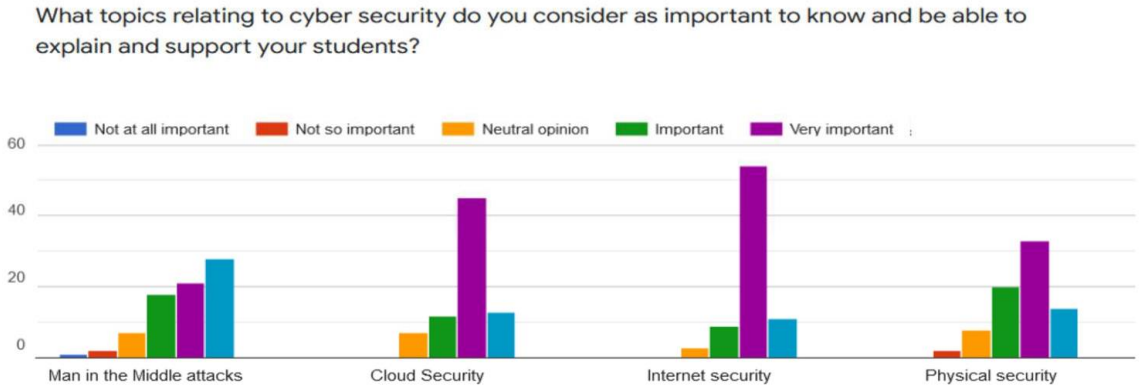


Figure 9 - What topics relating to cyber security do you consider important to know and be able to explain and support your students (man in the middle attacks, cloud security, internet safety, physical security)

CybARverse

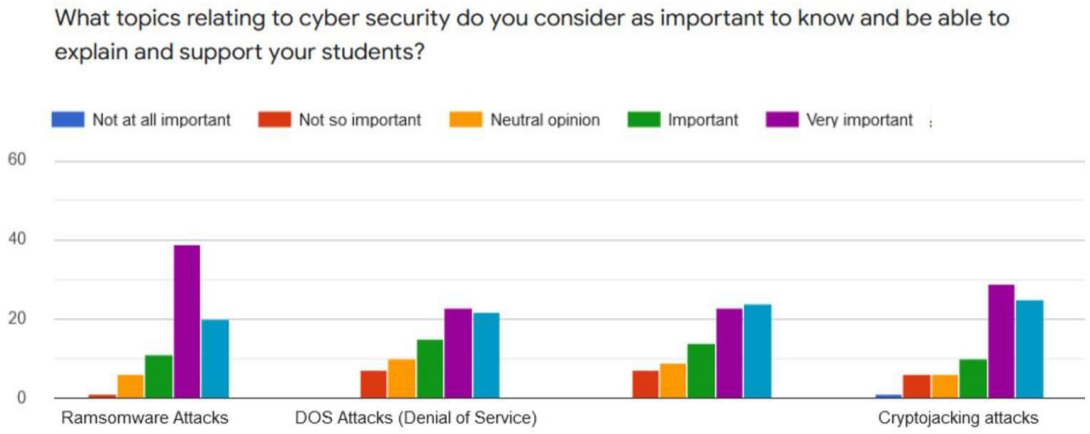


Figure 10 - What topics relating to cyber security do you consider important to know and be able to explain and support your students (ransomware attacks, DOS attacks, cryptojacking attacks)

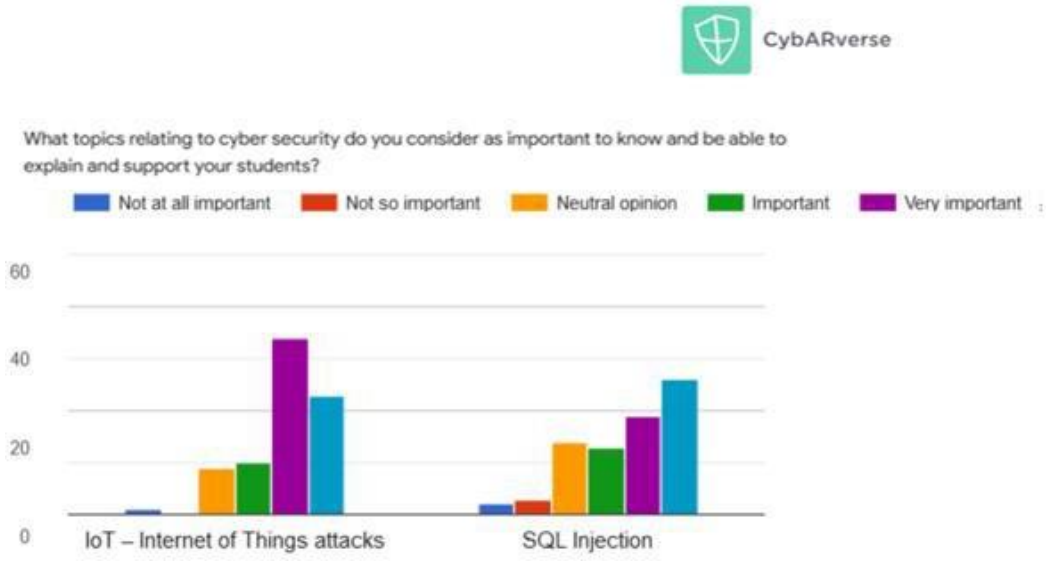


Figure 11 - What topics relating to cyber security do you consider important to know and be able to explain and support your students (IoT - internet of things attacks, SQL injection)

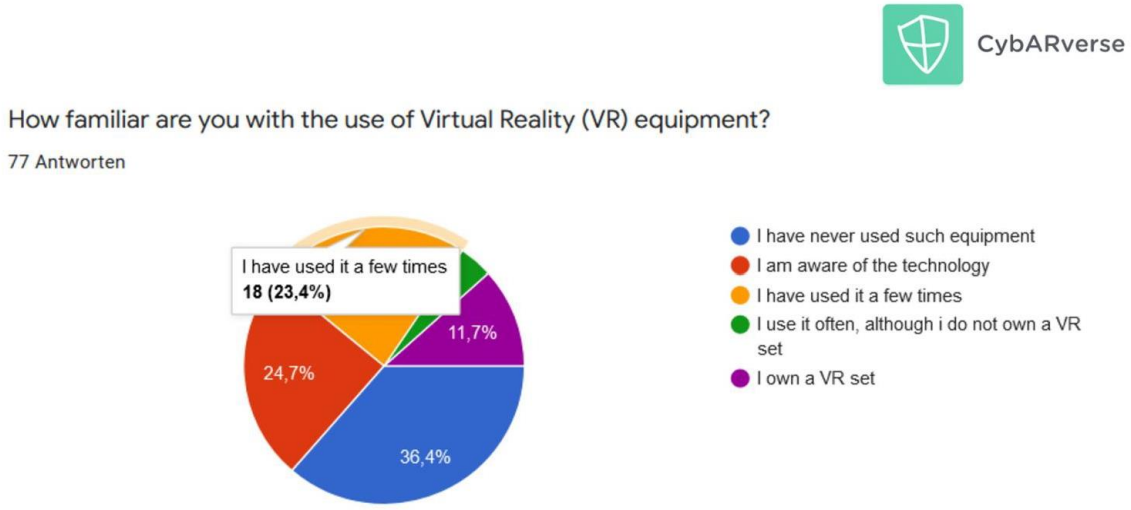


Figure 12 - How familiar are you with the use of Virtual Reality (VR) equipment?

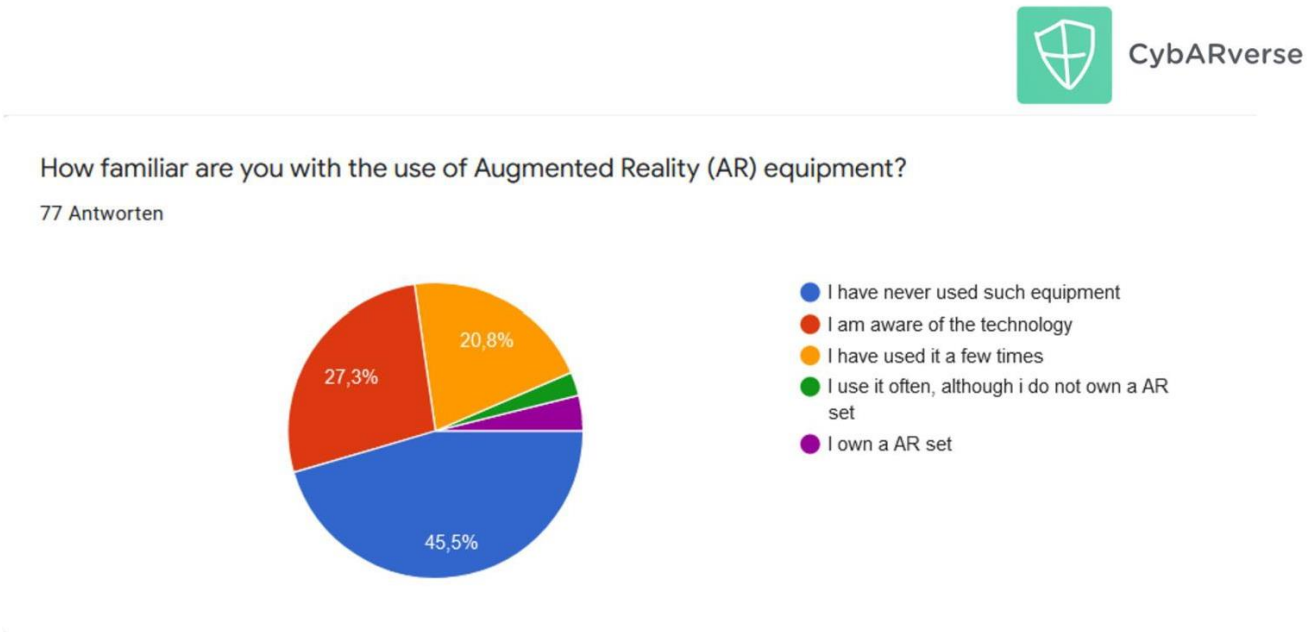


Figure 13 - How familiar are you with the use of Augmented Reality (AR) equipment?

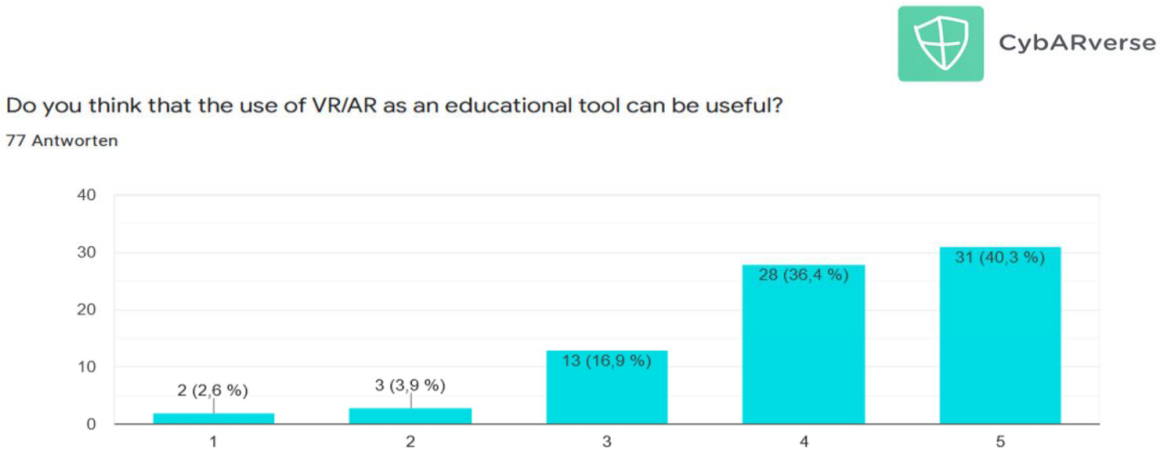


Figure 14 - Do you think that the use of VR/AR as an educational tool can be useful?

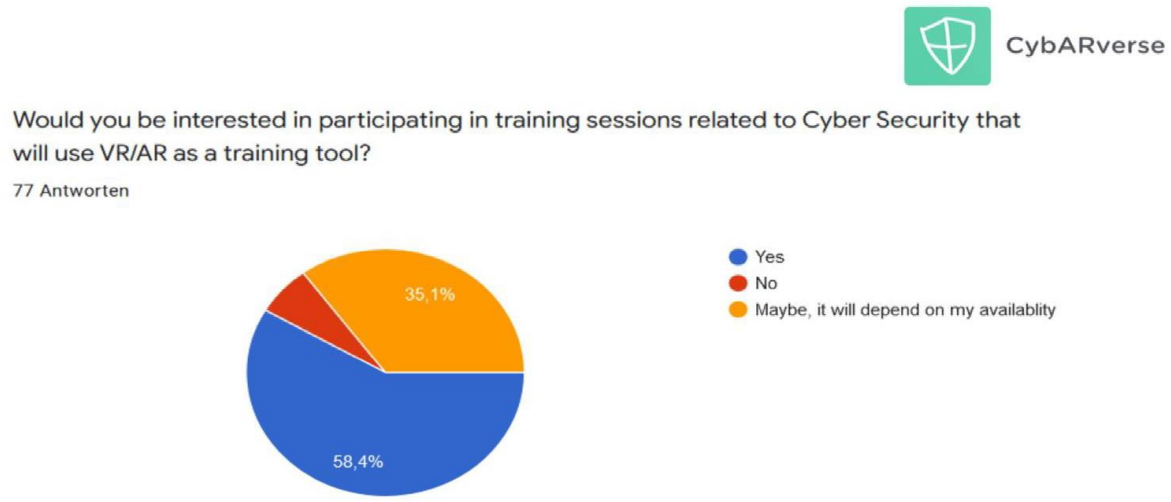


Figure 15 - would you be interested in participating in training sessions related to Cyber Security that will use VR/AR as a training tool?

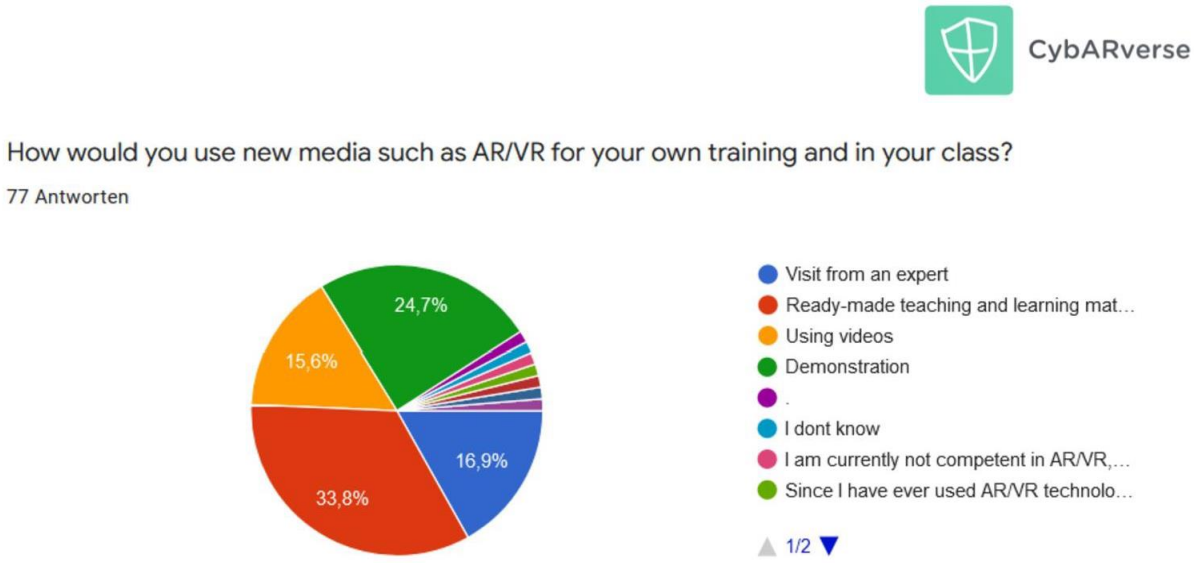


Figure 16 - How would you use new media such as AR/VR for your own training and in your class?

2.5 Development of learning objectives

Learning objectives are clear and specific statements about what VET educators should learn and understand by studying cybersecurity elements, what they are expected to learn and be able to do after completing the course or study programme.

Learning objectives are divided into three categories: knowledge, skills and attitudes. Knowledge refers to specific information that VET educators need to assimilate, such as terms, concepts and theories. Skills refer to the practical skills that they need to acquire, such as the ability to apply knowledge in a given context or to use specific technologies. Attitudes refer to values and behaviours that educators need to develop, such as critical thinking or the ability to work in a team.

Learning objectives must be specific, measurable, achievable, relevant and have a deadline. They should define the behaviours, abilities, and knowledge that learners will gain from studying the discipline so that they can be properly assessed.

The learning objectives for obtaining basic cybersecurity skills of IT and non-IT educators who teach at VET vocational schools are:

a) Identify cyber threats and vulnerabilities in communication systems and networks.

This competence refers to the ability to identify cyber threats and vulnerabilities in information systems and communication networks, using a variety of analysis techniques and tools. This may include network traffic analysis, vulnerability scanning, source code security analysis, and other security testing methods.

To achieve this specific learning goal, educators need to be familiar with the different types of cyber threats and understand how they can be used to exploit vulnerabilities in information systems and communication networks. They should also be able to use specific tools and techniques to identify and analyse cyber threats and vulnerabilities in communication systems and networks.

b) Apply cybersecurity principles and best practices to protect information systems and data against cyber-attacks.

This competence aims to develop the skills and knowledge necessary to assess and apply cybersecurity principles and techniques, as well as best practices for protecting information systems and data against cyber-attacks.

c) Acquire the knowledge and skills necessary for conducting cyber risk assessments and designing effective incident response plans aimed at minimizing the impact of cyberattacks.

Understanding and identifying cyber risks in a business environment, including internal and external threats, as well as vulnerabilities in information systems and communication networks, as well as the ability to develop incident response plans that reduce damage in the event of a cyberattack. These plans include incident identification steps, risk assessment, damage mitigation, restoration of services, and investigation of the incident. In addition, there should be clear procedures for communicating and reporting the incident so that it can be managed as efficiently and quickly as possible.

In general, this specific learning objective aims to provide educators with the necessary skills and knowledge to be able to assess cyber risks and develop effective incident response plans. These skills are crucial to protect computer systems and data from cyber-attacks and minimise damage in the event of a cybersecurity incident.

d) Develop data analysis skills and use security monitoring tools to detect suspicious activity in communication networks.

The development of data analysis skills and the use of security monitoring tools are essential in cybersecurity, as they allow the detection of suspicious activity in communication networks and the prevention of possible cyber-attacks.

Data analytics refers to the process of identifying and extracting relevant information from available data in order to gain a deeper understanding of the activity in communication networks. In cybersecurity, this process involves the analysis of system logs, security events and other relevant data to identify suspicious activities.

Security monitoring tools are specialised software programs that are designed to monitor network traffic and detect unauthorised or suspicious activity. These tools can be configured to automatically alert system administrators when they detect suspicious activities, such as unauthorised access attempts or downloads of files infected with viruses.

The development of data analysis skills and the use of security monitoring tools is done through training courses and practical training, which teach educators to interpret the collected data and take appropriate measures to protect communication networks from cyber-attacks.

e) Understanding the legal and ethical aspects related to cybersecurity and the social impact of cyber-attacks.

Understanding legal and ethical issues related to cybersecurity is an important aspect of cybersecurity competencies. First, it is important to understand the relevant legislation and regulations related to cybersecurity in order to ensure compliance and avoid possible negative legal consequences. It is also important to understand the professional ethics regarding cybersecurity, including the responsibility and confidentiality of information.

It is also important to understand the social impact of cyber-attacks and how they can affect communities and society as a whole. Cyber-attacks can have serious consequences, such as loss of personal and financial data, privacy violations, blackmail, etc. They can affect not only individuals and organisations, but also critical infrastructures such as energy and communication networks, which can have a negative impact on the economy and national security. Therefore, understanding the social impact of cyber-attacks and the role that cybersecurity plays in protecting society is essential to develop effective skills in this area.

3 LEARNING MATRICES

Bloom's Taxonomy is a framework for categorising educational goals and objectives. It was first developed by educational psychologist Benjamin Bloom in 1956 and has since been revised by other scholars. The taxonomy organises educational objectives into three domains: cognitive, affective, and psychomotor. The cognitive domain focuses on intellectual skills such as knowledge, comprehension, application, analysis, synthesis, and evaluation. The affective domain focuses on emotional and social

skills such as attitudes, values, and interpersonal relationships. The psychomotor domain focuses on physical skills such as coordination, dexterity, and manipulation.

Each of these domains is further subdivided into specific levels or categories that describe increasingly complex types of learning. For example, in the cognitive domain, the levels range from simple recall of information to more complex activities such as applying or evaluating that information.

The Bloom's Taxonomy framework is widely used in education to help teachers and learners set and achieve appropriate learning goals and objectives. By using the taxonomy to structure lesson plans, educators can ensure that their teaching addresses a range of different learning needs and styles, and that educators are able to progress through increasingly complex levels of understanding and skill.

Considering the survey conducted among IT and non-IT teachers from the 4 countries: LT, CY, RO, and MT, we generated learning matrices using Bloom's taxonomy for the main topics of interest specified by them.

Assessment: To evaluate educators' understanding and application of the lesson content, various assessment methods will be utilised. Formative assessments will include in-class group discussions, case study analyses, and hands-on VR simulations, which will allow educators to demonstrate their grasp of cybersecurity concepts and the use of immersive technologies in cybersecurity teaching. A summative assessment will consist of a short quiz or written reflection, requiring educators to define key terms, explain and discuss the role of VR and AR in detecting, preventing, and responding to such exploits. Additionally, peer assessment during group activities will encourage educators to evaluate their own and their peers' performance, fostering collaborative learning and critical thinking skills.

In analogy to the periodic table of elements, for providing a logical order and classification of chemical elements, the cybersecurity trainings are ordered similar in:

a) Rows: increasing complexity of attacks (to identify and react)
b) Columns: similar type of attacks

In reference to the DigCompEdu Framework, the newcomer (A1) until the expert level (B2) is represented. A1-B1 represents the cybersecurity awareness trainings for encouraging and implementing relevant measures among teachers/trainers and learners. The expert level represents the cybersecurity literacy trainings and the derived pedagogical needs.

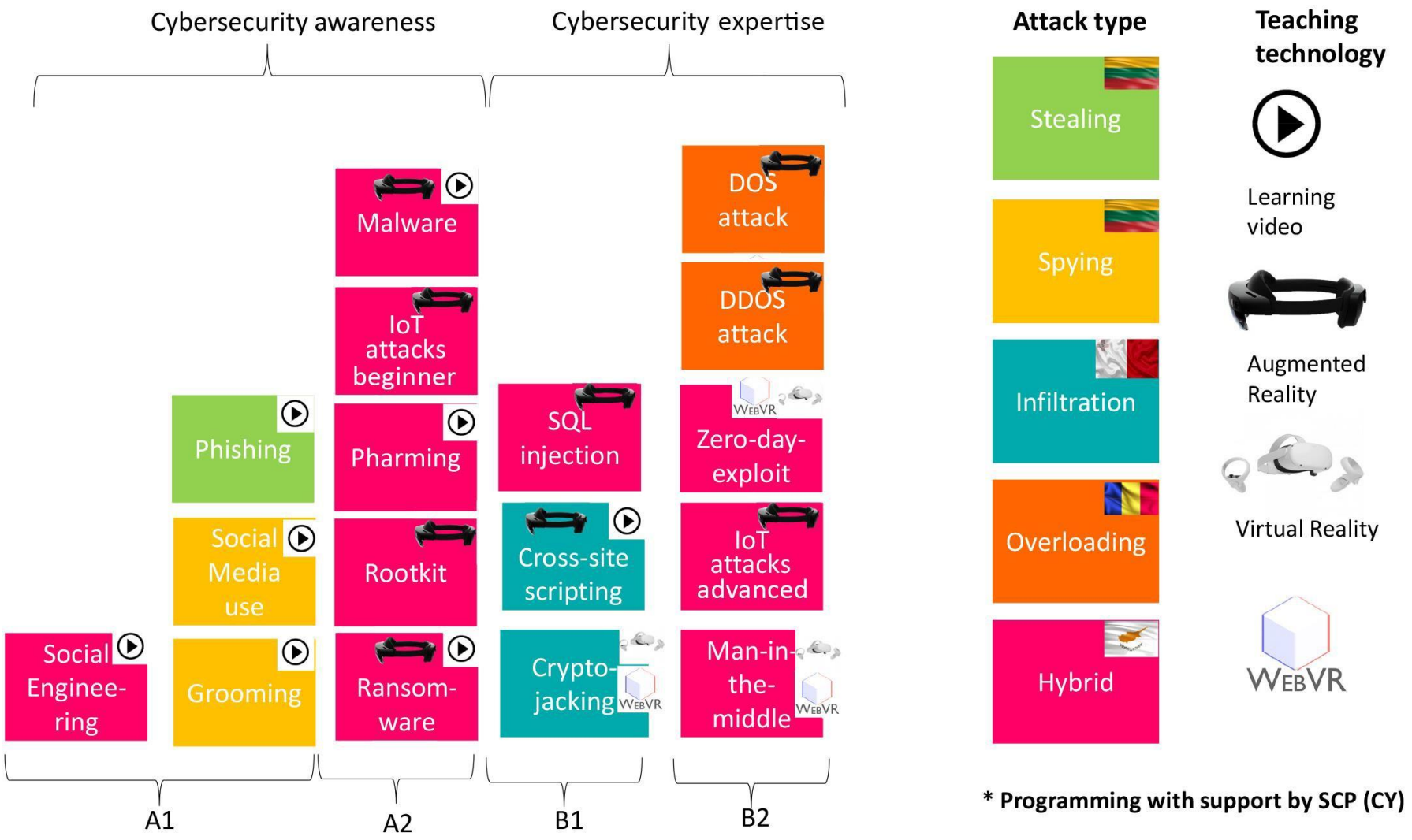


Figure 17 - Cybersecurity levels (Cybersecurity awareness/ Cybersecurity expertise)

3.1 A1 / Social engineering

Social engineering is a type of cyberattack that relies on psychological manipulation to trick individuals into divulging sensitive information, performing actions that compromise security, or giving access to restricted areas or data. Social engineering attacks are designed to exploit human weaknesses rather than technical vulnerabilities. Examples of social engineering attacks include phishing emails, pretexting (creating a false scenario to obtain sensitive information), baiting (offering something in exchange for sensitive information), and spear phishing (targeted phishing attacks).

Learning objectives:

1. Understand the concept of social engineering
2. Learn the different types of social engineering attacks
3. Understand the human vulnerabilities that social engineering attacks exploit
4. Learn how to prevent and mitigate social engineering attacks

Table 1: Social engineering Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the concept and methods of social engineering	- Define what social engineering is and its purpose - Identify common social engineering techniques and tactics - Explain the psychological principles used in social engineering attacks
Analyzing	Analyze real-world examples of social engineering attacks	- Examine case studies of successful social engineering attacks - Analyze the strategies employed by attackers to manipulate human behavior - Identify the vulnerabilities exploited in social engineering attacks
Evaluating	Evaluate the impact and consequences of social engineering attacks	- Assess the financial, reputational, and operational impact of social engineering incidents - Evaluate the effectiveness of security measures in preventing and mitigating social engineering attacks - Compare and contrast different strategies for social engineering prevention and awareness

3.2 A1 / Phishing

Phishing is a type of cyber-attack where attackers use fraudulent emails, instant messages, or other forms of electronic communication to trick individuals into providing sensitive information such as login credentials, credit card numbers, or personal data. These messages may appear to be from a legitimate source such as a bank, social media platform, or online retailer, but they are actually designed to steal personal information or infect a user's computer or network with malware. The goal of phishing attacks is to deceive the victim into divulging their sensitive information, which can then be used for identity theft, financial fraud, or other malicious purposes. Phishing attacks can be carried out through a variety of techniques, such as spear phishing, whaling, and clone phishing.

Learning objective:

1. Understand the concept of Phishing
2. Learn about the different types of phishing
3. Educators will be able to design effective measures to prevent Phishing attacks.

Table 2: Phishing Matrix

Bloom's Taxonomy	**Learning Outcome**	**Learning Units**
Understanding	Understand the concept and techniques used in phishing	- Define what phishing is and its basic characteristics - Differentiate between phishing, pharming, and other cyber-attack techniques - Identify common phishing methods such as email phishing, spear phishing, and smishing
Analyzing	Analyze the tactics and impact of phishing attacks	- Analyze real-world examples of phishing attacks and their consequences - Study the social engineering techniques used by attackers to deceive and manipulate victims - Investigate the methods employed to trick users into revealing sensitive information
Evaluating	Evaluate the effectiveness of prevention and detection measures for phishing attacks	- Evaluate the role of user awareness and education in preventing phishing incidents - Assess the effectiveness of email filters, spam detection, and anti-phishing tools - Compare and contrast different anti-phishing strategies and technologies

3.3 A1 / Social media

Social media threats refer to the risks and dangers that arise from using social media platforms. These threats can include cyberbullying, online harassment, identity theft, phishing, malware attacks, and the spread of misinformation or fake news. Social media threats can impact individuals, businesses, and society as a whole, and they can result in serious consequences such as reputation damage, financial loss, and even physical harm. Therefore, it is essential to understand and be aware of the various social media threats and take appropriate measures to mitigate them.

Learning objective:

1. Understand the concept of social media
2. Learn the different types of social media attacks
3. Understand the human vulnerabilities that social media attacks exploit
4. Learn how to prevent and mitigate social media attacks.

Table 3: Social media threats Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the cybersecurity risks associated with social media	- Explore common cybersecurity threats and vulnerabilities related to social media - Identify potential risks and consequences of social media usage - Understand the importance of protecting personal information online
Analyzing	Analyze the impact of social media on cybersecurity	- Examine real-world examples of cyber-attacks and privacy breaches through social media - Analyze the techniques used by attackers to exploit social media platforms - Identify the potential consequences of compromised social media accounts
Evaluating	Evaluate the best practices for securing social media accounts and mitigating cybersecurity risks	- Assess the importance of strong passwords, two-factor authentication, and privacy settings - Evaluate the effectiveness of security measures in preventing social media-related threats - Identify strategies for educating and raising awareness about cybersecurity risks in social media - Evaluate the ethical considerations of social media cybersecurity and the responsibilities of social media platforms in ensuring user privacy and data protection

3.4 A1 / Grooming

Grooming is a term used to describe the process by which an attacker builds a relationship with their victim in order to gain their trust and exploit their vulnerabilities for malicious purposes. In the context of cybersecurity, grooming is often used to describe the tactics used by attackers to trick individuals into divulging sensitive information or installing malware on their devices.

Learning objective:

1. Understand what a Grooming attack is and how it works.
2. To know the most common techniques used in Grooming attacks.
3. Be able to identify the signs of a Grooming attack.
4. Know how to protect against a Grooming attack.

Table 4: Grooming Matrix

Bloom's Taxonomy	**Learning Outcome**	**Learning Units**
Understanding	Understand the concept and tactics used in grooming	- Define what grooming is and its characteristics - Identify common tactics and strategies employed by groomers -Analyze the psychological and emotional manipulation techniques used in grooming
Analyzing	Analyze the impact of grooming on victims	- Examine case studies or real-life examples of grooming incidents - Investigate the role of online platforms and social media in facilitating grooming activities
Evaluating	Evaluate the effectiveness of prevention and intervention strategies	- Analyze the importance of early detection and reporting in preventing grooming incidents - Compare and contrast different intervention approaches and their effectiveness in supporting grooming victims

3.5 A2 / Malware

A malware attack refers to a malicious software that is designed to cause harm to computer systems, networks, or devices. Malware can be programmed to execute a range of harmful actions, such as stealing sensitive information, encrypting files, disrupting system operations, or using infected devices to launch further attacks. Malware attacks can be initiated through a variety of means, including email attachments, malicious websites, infected software, or vulnerable network connections. Due to the widespread use of computer systems and the internet, malware attacks pose a significant threat to organizations and individuals alike, and cybersecurity professionals must work to develop effective strategies for preventing, detecting, and responding to these types of attacks.

Learning objectives:

1. Understand the concept of malware
2. Learn about the different types of malware
3. Learn how to prevent and mitigate malware attacks

Table 5: Malware Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the concept and types of malware	- Define what malware is and its basic characteristics - Identify different types of malware such as viruses, worms, trojans, ransomware, etc. - Explain how malware can infiltrate systems and devices
Analyzing	Analyze the impact and behavior of malware	- Analyze real-world examples of malware attacks and their consequences - Study the propagation methods of different types of malware
Evaluating	Evaluate the effectiveness of malware detection and prevention strategies	- Evaluate different antivirus and anti-malware software solutions - Analyze the role of firewalls, intrusion detection systems, and other security measures in preventing malware infections - Compare and contrast different malware detection and removal techniques

3.6 A2 / IoT (Internet of Things) beginners

IoT (Internet of Things) attacks refer to malicious activities aimed at exploiting vulnerabilities in the interconnected devices and systems that make up the IoT ecosystem. These attacks can take various forms, such as unauthorised access, data theft, malware infections, and denial-of-service (DoS) attacks, among others. Since IoT devices are often designed with minimal security measures, they can be vulnerable to attack and can be used as entry points into larger networks. IoT attacks can target a wide range of devices, including smart home appliances, industrial equipment, medical devices, and more.

Learning objectives:

1. Understand what IoT (Internet of Things) is and how it works
2. Learn about different types of IoT attacks and how they work
3. Understand the potential consequences of IoT attacks
4. Explore ways to prevent IoT attacks

Table 6: IoT attacks Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Remembering	Define IoT and its fundamental concept.	- Define what IoT attacks are and their basic characteristics - Methods and techniques used in IoT attacks
Understanding	Explain the concept of the Internet of Things and its significance.	- Identify common examples of IoT attacks using AR -Understand the significance and potential impact of IoT in various fields
Analyzing	Analyze the impact of grooming on victims	- Examine real-world examples of IoT attacks and their consequences - Assess the financial, privacy, and safety implications of IoT attacks
Evaluating	Analyze the impact of IoT attacks	- Evaluate the potential consequences of IoT attacks - Compare and contrast different security measures for protecting against IoT attacks

3.7 A2 / Pharming

Pharming attack is a type of cyber-attack that involves the exploitation of DNS (Domain Name System) servers to redirect legitimate website traffic to a malicious website, which appears to be legitimate. In a pharming attack, the attacker compromises the DNS server or the user's computer to modify the DNS records, allowing them to redirect the user to a fake website that can collect sensitive information such as login credentials, credit card numbers, and other personal information.

Learning objective:

1. Understand the concept of Pharming
2. Learn about the different types of Pharming
3. Learn how to prevent and mitigate Pharming attacks

Table 7: Pharming Attack Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the concept and techniques used in pharming	- Define what pharming is and its basic characteristics - Differentiate between phishing and pharming attacks - Identify the methods used by attackers to manipulate DNS settings or compromise user systems for pharming
Analyzing	Analyze the impact and methods of pharming attacks	- Analyze real-world examples of pharming attacks and their consequences Study the techniques employed by attackers to redirect website traffic and deceive users Investigate the vulnerabilities in the DNS infrastructure that can be exploited for pharming
Evaluating	Evaluate the effectiveness of prevention and detection measures for pharming attacks	- Evaluate the role of secure DNS protocols such as DNSSEC in preventing DNS manipulation - Assess the effectiveness of DNS monitoring and anomaly detection techniques - Compare and contrast different DNS service providers and their security features

3.8 A2 / Rootkit

A rootkit is a type of malicious software designed to conceal its presence and activities on a computer or network. Rootkits are often used to gain unauthorized access to a system, steal data, or launch other types of attacks. Rootkits are particularly difficult to detect because they operate at the lowest levels of the operating system, making them invisible to standard security software such as antivirus programs. They can be installed on a system through a variety of methods, including email attachments, malicious websites, or software vulnerabilities.

Learning objectives:

1. Understand the concept of rootkit
2. Learn about the different types of rootkit
3. Learn how to prevent and mitigate rootkit attacks

Table 8: Rootkit Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the concept and characteristics of rootkits	- Define what a rootkit is and how it operates - Identify the key features and purpose of rootkits - Explain the common methods used for rootkit installation and persistence
Analyzing	Analyze the impact and behavior of rootkits	- Analyze real-world examples of rootkit attacks and their consequences - Study the techniques employed by rootkits to hide their presence and evade detection - Investigate the potential vulnerabilities that rootkits exploit
Evaluating	Evaluate the effectiveness of prevention and detection measures for rootkits	- Evaluate the role of secure boot mechanisms and firmware protection in preventing rootkit infections - Assess the effectiveness of rootkit detection tools and techniques - Compare and contrast different strategies for rootkit prevention and removal

3.9 A2 / Ransomware

Ransomware is a type of malicious software that encrypts files on a victim's computer or network, making them inaccessible until a ransom is paid. Ransomware attacks typically begin with an email or other form of communication that appears to be legitimate, containing an infected attachment or link that, when clicked, executes the malware. Once the malware is installed, it begins encrypting files and folders, rendering them inaccessible to the user. The attackers then demand payment in exchange for a decryption key to unlock the files. Ransomware attacks can cause significant damage, resulting in data loss, financial loss, and reputational damage. They can also be challenging to detect and mitigate, making them a persistent threat to organizations and individuals alike.

Learning objective:

1. Understand the concept of Ransomware
2. Learn about the different types of Ransomware
3. Learn how to prevent and mitigate Ransomware attacks

Table 9: Ransomware Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the concept and characteristics of ransomware	- Define what ransomware is and how it operates - Identify the key features and components of ransomware attacks - Explain the common methods used for ransomware distribution and infection
Analyzing	Analyze the impact and behavior of ransomware	- Analyze real-world examples of ransomware attacks and their consequences - Study the encryption mechanisms employed by ransomware - Investigate the tactics used by attackers to demand and collect ransom payments
Evaluating	Evaluate the effectiveness of prevention and mitigation measures for ransomware attacks	- Evaluate the role of robust backup and disaster recovery strategies in mitigating ransomware incidents - Compare and contrast different strategies for ransomware prevention and incident response

3.10 B1 / SQL injection

SQL injection is a type of cyber-attack in which an attacker exploits vulnerabilities in a website or web application that allows them to insert malicious SQL code into a SQL statement. SQL (Structured Query Language) is a programming language used to communicate with databases to retrieve, update, or modify data.

Learning objective:

1. Understand the concept of SQL injection
2. Learn the different types of SQL injections attacks
3. Understand the vulnerabilities that SQL injection attacks exploit
4. Learn how to prevent and mitigate SQL injections attacks

Table 10: SQL Injection Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the concept and risks of SQL injection attacks	- Define what SQL injection is and how it can be exploited - Identify the potential consequences of SQL injection attacks - Understand the role of user input in SQL injection vulnerabilities
Analyzing	Analyze real-world examples of SQL injection attacks	- Examine case studies of successful SQL injection attacks - Analyze the techniques used by attackers to exploit SQL vulnerabilities - Identify the potential impact of SQL injection on databases and systems
Evaluating	Evaluate the best practices for preventing SQL injection attacks	- Assess the importance of input validation and sanitization in preventing SQL injection - Evaluate the effectiveness of parameterized queries and prepared statements - Identify strategies for secure coding practices to mitigate SQL injection risks

3.11 B1 / Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a type of security vulnerability that allows an attacker to inject malicious code into a web page viewed by other users. This is done by exploiting vulnerabilities in a website's code, allowing the attacker to inject scripts or other code that can steal sensitive information, modify the appearance of the page, or perform other malicious actions. XSS attacks are particularly dangerous because they can be used to target multiple users at once and can be difficult to detect and prevent.

Learning objectives:

1. Educators will be able to define Cross-Site Scripting (XSS) and explain how it works.
2. Educators will be able to identify different types of XSS attacks and explain their potential risks.
3. Educators will be able to describe methods for preventing XSS attacks.
4. Educators will be able to evaluate vulnerabilities associated with XSS attacks and suggest ways to improve security.

Table 11: Cross-Site Scripting (XSS) Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Understanding	Understand the concept and risks of XSS attacks	- Define what XSS (Cross-Site Scripting) is and how it can be exploited - Identify the potential consequences of XSS attacks - Understand the different types of XSS vulnerabilities
Analyzing	Analyze real-world examples of XSS attacks	- Examine case studies of successful XSS attacks - Analyze the methods used by attackers to execute XSS attacks - Identify the potential impact of XSS on web applications and users
Evaluating	Evaluate the best practices for preventing XSS attacks	- Assess the importance of input validation and output encoding in preventing XSS - Evaluate the effectiveness of secure coding practices to mitigate XSS vulnerabilities - Identify strategies for educating developers and users about XSS risks and prevention measures

3.12 B1 / Cryptojacking

Cryptojacking, also known as malicious cryptocurrency mining, is a form of cyber-attack in which hackers use someone else's computer resources to mine cryptocurrencies without their knowledge or consent. This is typically done by infecting a victim's computer with malware that uses its processing power to mine cryptocurrency for the attacker. The victim may notice that their computer is running more slowly than usual, and they may also experience a shorter lifespan of their device due to the high amount of processing power being used. Cryptojacking can occur on both personal and business computers, and it has become increasingly prevalent as cryptocurrencies have gained popularity.

Learning objectives:

1. Educators will be able to define crypto jacking and identify its impact on computer systems and users.
2. Educators will be able to explain how cryptojacking works and how it can be prevented.
3. Educators will be able to analyse real-world examples of cryptojacking attacks and their consequences.

Table 12: Cryptojacking Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Remembering	Recall the concept of Cryptojacking	- Define what Cryptojacking is and its basic characteristics - Identify common examples of Cryptojacking attacks using VR/Webvr - Recognize the potential impact of Cryptojacking attacks
Understanding	Understand how Cryptojacking works	- Study the mechanisms and techniques used in Cryptojacking attacks - Explore different types of Cryptojacking methods and their variations
Analysing	Analyze the impact of Cryptojacking	- Examine real-world examples of Cryptojacking attacks and their consequences - Assess the financial, operational, and reputational impact of Cryptojacking attacks
Evaluating	Evaluate the effectiveness of Cryptojacking prevention techniques	- Evaluate the potential consequences of Cryptojacking attacks - Compare and contrast different prevention techniques for Cryptojacking

3.13 B2 / DoS (Denial of Service) attack

A DoS (Denial of Service) attack is a type of cyber-attack that involves overwhelming a targeted server or network with a flood of traffic from a single source, thereby rendering it inaccessible to legitimate users.

Learning Objectives:

1. Understand what a DoS attack is and how it works.
2. To know the most common techniques used in DoS attacks.
3. Be able to identify the signs of a DoS attack.
4. Know how to protect against a DoS attack.

Table 13: DOS Attack Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Remembering	Recall the concept of DoS attacks	- Define what a DoS attack is and its basic characteristics - Identify common examples of DoS attacks - Recognize the potential impact of DoS attacks
Understanding	Understand how DoS attacks work	- Study the methods and techniques used in DoS attacks - Explore different types of DoS attacks and their characteristics
Analysing	Analyze the impact of DoS attacks	- Examine real-world examples of DoS attacks and their consequences - Assess the financial, operational, and reputational impact of DoS attacks
Evaluating	Evaluate the effectiveness of DoS mitigation techniques	- Evaluate the potential consequences of DoS attacks - Compare and contrast different mitigation techniques for DoS attacks

3.14 B2 / DDoS (Distributed Denial of Service)

A DDoS (Distributed Denial of Service) attack is a type of cyber-attack where many computers, often controlled by a single attacker or group of attackers, attempt to overwhelm a targeted website, server, or network with a flood of traffic or requests. The goal of a DDoS attack is to disrupt or disable the targeted system, making it inaccessible to legitimate users.

Learning objective:

1. Understand what a DDoS attack is and how it works.
2. To know the most common techniques used in DDoS attacks.
3. Be able to identify the signs of a DDoS attack.
4. Know how to protect against a DDoS attack.

Table 14: DDoS Attack Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Remembering	Recall the concept of DDoS attacks	- Define what a DDoS attack is and its basic characteristics - Identify common examples of DDoS attacks - Recognize the potential impact of DDoS attacks
Understanding	Understand how DDoS attacks work	- Study the methods and techniques used in DDoS attacks - Explore different types of DDoS attacks and their characteristics
Analysing	Analyze the impact of DDoS attacks	- Examine real-world examples of DDoS attacks and their consequences - Assess the financial, operational, and reputational impact of DDoS attacks
Evaluating	Evaluate the effectiveness of DDoS mitigation techniques	- Evaluate the potential consequences of DDoS attacks - Compare and contrast different mitigation techniques for DDoS attacks

3.15 B2 / A zero-day exploit

A zero-day exploit attack is a type of cyber-attack that takes advantage of a security vulnerability in software or hardware before the developer or vendor has a chance to release a patch or update to fix the problem. Zero-day exploits are considered highly effective and dangerous because they are unknown to the public and the victim, which means there is no protection or defence available against them.

Learning objectives:

1. Define what zero-day exploits are and how they work.
2. Identify the different types of zero-day exploits and the impact they can have on businesses and organisations.
3. Understand the techniques used by attackers to find zero-day vulnerabilities.
4. Analyse strategies for detecting and mitigating zero-day exploits.
5. Explore ethical and legal considerations surrounding zero-day exploits.

Table 15: Zero-Day Exploits Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Remembering	Recall the concept of zero-day exploits	- Define what zero-day exploits are and their basic characteristics - Identify common examples and scenarios where zero-day exploits can occur - Recognize the potential risks and consequences of zero-day exploits
Understanding	Understand how zero-day exploits work	- Study the vulnerabilities and techniques used in zero-day exploits - Explore the life cycle of a zero-day exploit and its impact
Analysing	Analyze the impact of zero-day exploits	- Examine real-world examples of zero-day exploit incidents and their consequences - Assess the financial, privacy, and security implications of zero-day exploits
Evaluating	Evaluate the effectiveness of zero-day exploit prevention techniques	- Evaluate the potential consequences of zero-day exploits - Compare and contrast different prevention techniques and strategies for mitigating zero-day exploits

3.16 B2 / IoT (Internet of Things) advanced

IoT (Internet of Things) attacks refer to malicious activities aimed at exploiting vulnerabilities in the interconnected devices and systems that make up the IoT ecosystem. These attacks can take various forms, such as unauthorised access, data theft, malware infections, and denial-of-service (DoS) attacks, among others. Since IoT devices are often designed with minimal security measures, they can be vulnerable to attack and can be used as entry points into larger networks. IoT attacks can target a wide range of devices, including smart home appliances, industrial equipment, medical devices, and more.

Learning objectives:

1. Learn about different types of IoT attacks and how they work
2. Understand the potential consequences of IoT attacks
3. Analyze the intricate interactions and dependencies among various components in complex IoT architectures, considering edge, fog, and cloud computing paradigms
4. Explore ways to prevent IoT attacks

Table 16: IoT attacks Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Remembering	Recall the concept of IoT attacks	- Define what IoT attacks are and their characteristics - Identify examples of IoT attacks using AR
Understanding	Understand how zero-day exploits work	- Methods and techniques used in IoT attacks - Explore different types of IoT attacks and their impact
Analysing	Understand how IoT attacks work	- Examine real-world examples of IoT attacks and their consequences - Visualize the data using charts, graphs, and plots to identify initial patterns and trends.
Evaluating	Evaluate the effectiveness of zero-day exploit prevention techniques	- Identify potential security risks specific to IoT devices, such as unauthorized access, data breaches, device manipulation, and privacy violations. - Impact and likelihood of each risk to prioritize mitigation efforts

3.17 B2 / Man-in-the-middle (MITM)

Man-in-the-middle (MITM) attack is a type of cyber-attack in which an attacker intercepts the communication between two parties and alters or injects new messages in the communication stream, without the knowledge or consent of either party. The attacker secretly relays and possibly alters the communication between the two parties, in a way that they believe they are still communicating with each other directly. The goal of a MITM attack is usually to steal sensitive information, such as login credentials, financial information, or personal data. MITM attacks can be carried out on any type of communication, including email, instant messaging, voice over IP (VoIP), and even secure HTTPS connections.

Learning objective:

5. Understand the concept of MITM
6. Learn about the different types of MITM
7. Learn how to prevent and mitigate MITM attacks

Table 17: Man-in-the-Middle Attacks Matrix

Bloom's Taxonomy	Learning Outcome	Learning Units
Remembering	Recall the concept of Man-in-the-Middle attacks	- Define what a Man-in-the-Middle attack is and its basic characteristics - Identify common examples and scenarios where MitM attacks can occur - Recognize the potential risks and consequences of MitM attacks
Understanding	Understand how Man-in-the-Middle attacks work	- Study the techniques and methods used in MitM attacks - Explore different types of MitM attacks and their implications
Analysing	Analyze the impact of Man-in-the-Middle attacks	- Examine real-world examples of MitM attacks and their consequences - Assess the financial, privacy, and security implications of MitM attacks
Evaluating	Evaluate the effectiveness of MitM prevention techniques	- Evaluate the potential consequences of MitM attacks - Compare and contrast different prevention techniques and tools for mitigating MitM attacks

We will be utilizing these technologies on our 16 carefully curated learning scenarios on WP3, where it is found the more appropriate and pedagogical sound to help trainers become more cyber-aware and, at the same time to be able to train in their classrooms the different cybersecurity levels (awareness/literacy) found on the 16 learning scenarios.

To enhance the learning experience of VET educators, we are deploying XR technologies such as Augmented Reality (AR), Virtual Reality (VR), and WebVR on the above matrices. Using these state-of-the-art tools, we aim to create an immersive and interactive training environment that enables career educators to understand complex cybersecurity concepts better.

Extended Reality (XR) is an umbrella term that encompasses various immersive technologies that extend or enhance human perception and interaction with the digital world. XR combines elements of virtual reality (VR), augmented reality (AR), and mixed reality (MR) to create a spectrum of experiences that range from fully immersive virtual environments to enhanced real-world experiences.

By integrating Extended Reality (XR), trainers can interact with computerized data and cyber defense recreations in the virtual environment. This hands-on approach will empower them to imagine potential cyber dangers in a safe environment, engaging them to understand cybersecurity threats much better. Moreover, XR will immerse trainers in virtual situations to interact with cyber-attacks in a secure and controlled setting. By inundating themselves with these exact scenarios, trainers can become proactive in cyberattacks and increase their cybersecurity awareness skills.

4 BIBLIOGRAPHY

1. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape
2. National Institute of Standards and Technology (NIST) https://www.nist.gov/topics/cybersecurity
3. United States Computer Emergency Readiness Team (US-CERT): The official website of US-CERT provides a wealth of information on cybersecurity, including alerts, bulletins, and advisories related to cyber threats and attacks. Access it at: https://www.us-cert.gov/
4. MITRE ATT&CK: MITRE ATT&CK is a globally recognized knowledge base that provides detailed information on adversary tactics, techniques, and procedures (TTPs). It is an invaluable resource for understanding cyber-attacks. Visit: https://attack.mitre.org/
5. The Cybersecurity and Infrastructure Security Agency (CISA): CISA is a U.S. government agency that provides resources, alerts, and guidance related to cybersecurity threats and incidents. Explore their website at: https://www.cisa.gov/