iAware

Methodological Guide With Trainer Instructions

Erasmus+

UNIVERSIDADE LUSÓFONA

EuroForum

prism impresa sociale s.r.l.

Co-funded by the Erasmus+ Programme of the European Union

This publication has been funded with support from the European Commission. It reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Grant Agreement number: 2019-1-PL01-KA204-065601

Authors:

Piotr Celiński	**Euro-Forum**
Paulo Ferreira	**Universidade Lusófona**
Zbigniew Husak	**Euro-Forum**
Simone Indovina	**PRISM Impresa Sociale s.r.l.**
Beniamino Torregrossa	**PRISM Impresa Sociale s.r.l.**
Katarzyna Kopeć	**Euro-Forum**

Lublin, Poland, 2022

Euro-Forum Agnieszka Gudków, Marek Gudków Spółka Jawna

INTRODUCTION

Living in the modern world, personal development, as wellas undertaking professional activity all require an individual to possess certain basic competences that allow them to act effectively in specific conditions. The analysis of these necessary skills has resulted in the development of a list of key competences acquired through lifelong learning. In its Council Recommendations of 22 May 2018, the European Parliament lists digital competences among the eight key competences whose importance is increasing not only due to the very dynamic development of technology, but also due to the experience gained during the COVID-19 pandemic.

Digital competence, which involves the critical and responsible use of new technologies, has been recognised by the European Parliament as one of the key competences for lifelong learning and involves the critical and responsible use of new technologies. The definition of the term 'digital competence' is not straightforward and cannot be detailed because the digital world is constantly evolving. Digital competences are not a set of skills for the effective use of computers, mobile devices or the Internet, nor do they refer to specific solutions or tools, since the speed of change in the technological sphere would make them obsolete very quickly. What is more, digital competences are not limited to hardware skills alone, but they also include information competences, the ability to access information, use it and develop one's knowledge with the help of ICT. These competences facilitate further continuous development and, in that way, also adaptation to the requirements of the modern world.

It can be said that digital competences are as important in the 21st century as literacy or mathematical and linguistic competences. They are linked to many of the skills that citizens of modern Europe should possess and they directly influence the acquisition of other key competences such as communication in the mother tongue and foreign languages, ability to learn as well as social and civic competences. Digital literacy has an impact in areas such as quality of life, economy, health care, education, science, security, agriculture, culture, entertainment, and participation in society.

In this e-book, we aim to include a comprehensive training programme that was developed as part of the Erasmus+ project 'iAware -Innovative Programme for Digital Adult Education'. The project was implemented by three partner organisations from three different European countries. 'EURO-FORUM' from Poland was the project leader and 'Prism' from Italy and Lusofona University from Portugal were its partner organisations. The project is a response to the problem of insufficient digital competences among adults diagnosed jointly by these organisations. The aims of the project included:

- the creation of a modern ICT and adult education programme that takes into account modern challenges in terms of Internet safety and informed use of online resources
- provision of the right tools, knowledge resources and skills to ICT trainers and adult educators in order to shape adults' attitudes towards the informed use of modern technologies
- improvement of key digital competences of adults in the European Union and development of the information society

The programme that is presented in the following chapters and created as part of the 'iAware' project is divided into five thematic modules:

1. *Types and identification of online threats*
2. *Counteracting and minimising risks and ensuring online safety*
3. *Active participation in the information society*
4. *Making an informed use of information and communication technology*
5. *Development directions of the internet, active building of a global community of e-citizens*

The e-book is intended for ICT trainers and educators working with adults as a support resource and compendium for the use of the innovative method developed within the project. The following chapters will help trainers to comprehensively prepare for their work on the basis of the lesson plans developed in the 'iAware' project.

CHAPTER 1

-

PROBLEMS ARISING FROM TEACHING ICT TO LOW-COMPETENT ADULTS AND WAYS OF ADDRESSING THEM

The level of digital competence and the related quality of the use of digital tools is a key aspect of life in the 21st century society, which has implications both at a general level, affecting the labour market or economic development, influencing civic activity and the functioning of public institutions, as well as at a very specific level, affecting the quality of life of individual EU citizens. Nonetheless, the undoubted benefits of technological development are accompanied by new problems. The widespread use of technologies, their increasing possibilities and frequently also their indispensability in everyday life mean that people who fail to use them or have a low level of such skills are increasingly socially excluded. It is becoming important to have the right competences to use technology to their advantage.

Increasing the level of digital competence among adults has been a challenge posed to trainers working with the method from the 'iAware' project. Barriers related to computer and Internet use can be very different, among which we have technological factors related to the lack of technical possibilities to connect to the Internet, or finances, and psychological factors related to the lack of knowledge, motivation and appropriate skills to use.

The problems that can affect the teaching of low-skilled people can be divided into three areas:

1. *Problems related to lack of knowledge and motivation to use ICT resources*
2. *Problems related to lack of access to and opportunities for using ICT*
3. *Problems arising from lack of basic skills to use ICT tools effectively*

The above identified barriers to the use of ICT are interrelated and very commonly occur simultaneously.

PROBLEMS RELATED TO LACK OF KNOWLEDGE AND MOTIVATION TO USE ICT RESOURCES

Having the motivation to use new technologies is fundamental. Motivation is what determines decisions to buy a computer or a smartphone, to connect to the internet and to acquire the necessary skills to use relevant applications. Motivation is also key to using ICT solutions. Having access to computers and networks at home, work, school, as well as just using them is another issue, because having access to them does not necessarily mean using them straight away.

This phenomenon is related to a lack of motivation to use ICT solutions. A certain percentage of the population does not use the Internet, computers or mobile devices because they do by no means feel the need to do so. There are categories of people that include those who are digitally literate and yet refuse to use them. This is related to a lack of motivation due to a lack of knowledge of what the Internet can be used for, as well as to the ability to use it and the possibility to use by, e.g., family members who can search the Internet for information for the non-user. While the problem touches people of all ages, it is most often older people who are affected, which is often related to the perception that new technologies are only for young people, and the idea of lifelong learning is seen as strange and unnatural. There is a pattern that older people make less use of digital technologies, particularly the Internet. This is because digital technologies have been around for a short time and, as a novelty, are unfamiliar to this group of people and therefore less accessible. For the generations that have participated in IT classes at school from a very early age, using the benefits of the Internet is natural, and further functionalities such as online shopping or instant messaging are welcomed with enthusiasm. This is not so apparent for senior citizens.

Internet access alone does not guarantee that people will use it. What is key, however, is not the lack of willingness to use per se, but rather what the reasons for such reluctance there might be. These are the true barriers to digital uptake. At the core lies the problem of the lack of knowledge, which is an origin to other barriers and leads to a lack of need to use the Internet as well as to psychological barriers, including fear and self-exclusion through lack of motivation

to learn. The problem of lack of knowledge does not only involve ignorance of the possibilities offered by computers, smartphones and the Internet. It is also a lack of reliable information, which leads to a lack of trust in, e.g. online banking or information provided via the Internet. A lack of knowledge is also linked to the difficulty of finding topics and activities of interest to a person doing a search online, the acquisition of which would be a motivation to learn new skills. As a consequence, the lack of perception of the Internet and the computer as tools for satisfying one's own needs becomes a fundamental problem. A form of combating the key barrier – motivational exclusion – is to build the need to use the Internet around people's broader life, work, social or societal motivations. One way of counteracting this is through the participation of such people in courses or workshops organised by various organisations and aimed at specific audiences.

A significant barrier connected with starting to use digital technologies is the perception of those new technologies as a world to which one does not belong. This is often due to a passive attitude and an unwillingness to learn new things. There are also barriers related to fear, apprehension and various misconceptions associated with computer use, e.g. from computer addiction, from scammers or malware, or lack of faith in the ability to maintain social contacts over the Internet. Another problem that translates into a lack of motivation manifests in the lack of content and different services that could be of interest to specific groups. Overcoming these barriers is linked to the actions of content providers. It is not only about the actions of commercial companies, but also of government entities, e.g. adapting content and forms to people with disabilities. All the more so as access to the Internet is nowadays not only a convenience, but sometimes even a necessity for full participation in social or professional life.

PROBLEMS RELATED TO LACK OF ACCESS TO AND USE OF ICT

Problems related to lack of access include financial, network connection and hardware barriers. Financial barriers are mainly related to the lack of suitable equipment in the household and the lack of an Internet connection due to excessive prices. Another barrier related to lack of access is connected with the lack of technical feasibility of Internet delivery. This is especially true for residents of smaller towns, where there are sometimes insufficient funds to purchase computer equipment, and it is in vain to find modern technical solutions that would enable the use of all the possibilities of the Internet.

Nevertheless, in recent times, these problems have been losing relevance. This is mainly due to the development of infrastructure and the introduction of increasingly modern technologies, such as mobile Internet. The quality of Internet access – Internet bandwidth and reliability of the connection – is becoming more important. Digital activation cannot merely be about lowering access costs and setting up infrastructure; countries must make sure that all users have equal access. It is essential to continually make the public aware of the benefits of ICT use and local community activation efforts. For many people, simply because they have access to ICT does not mean that they will be active users. The right motivation needs to be fostered in these individuals and they need to be helped to increase their level of competence.

Another problem in using the Internet is linked to hardware limitations, which can be understood as the mismatch between hardware and software and the abilities of its users. This is particularly true for older people and people with disabilities. As the market develops, we are observing an increase in the availability of more intuitive technologies, tailored to specific user groups, e.g. appropriate key spacing on the keyboard, adapted screen resolution, font size, design and complexity of user interfaces, or choice of appropriate smartphone. Adapting web content, e.g. websites to allow older users or those with different disabilities, is counteracting this problem. Content made available on the web should be appropriate, useful and accessible to specific groups.

PROBLEMS ARISING FROM LACK OF BASIC SKILLS TO USE ICT TOOLS EFFECTIVELY

For some people who cannot use modern digital technologies, the lack of appropriate competences, but also the difficulty in acquiring new skills, is a limiting factor in starting to use the Internet. Even basic computer-related activities, such as switching on, typing, using a mouse, navigating websites or using a search engine, can be clearly difficult. At the same time, they are often insufficiently motivated to acquire new competences. A slower learning curve or the need for support from a more experienced and knowledgeable person to perform various activities, e.g. installing applications, performing registrations, learning to use the software, can also constitute a barrier.

When needs related to Internet or computer use do arise, they are reduced (e.g. dropping out of events for which one has to register online) or fulfilled by others. Competence barriers are often linked to a lack of confidence in one's own abilities, fear and, above all, the difficulty of identifying needs that can be met using the Internet. It is essential to encourage low-competent people to participate in training courses and workshops organised by different institutions or to acquire knowledge themselves.

CHAPTER 2

-

GOOD PRACTICES IN TEACHING ICT TO ADULTS

Nowadays, the dynamics of change can be observed, which concerns not only the technological and economic dimension, but also the societal dimension. Lifelong learning is taking on a special dimension, allowing us to function more easily in the surrounding, ever-changing reality. Learning is no longer just a voluntary activity undertaken by few individuals in order to satisfy their own ambitions, interests and personal development needs, but a necessity for proper functioning in social life and the labour market.

The most noticeable benefits of education include the knowledge and skills that an individual acquires throughout the learning process, especially when they result from the individual's own motivation and need. The competence gap is an equally essential reason for acquiring new competences. It refers to a state in which a person clearly feels the lack of a given skill. Through various developmental activities, the gap is filled and new skills open up new possibilities. Continuous competence development also has an impact on the mental sphere. Voluntary engagement in the learning process, especially regularity and consistence in action, builds up a person's sense of agency and influence. Delving into a topic that is interesting and inspiring contributes to a sense of satisfaction and increases the motivation to learn. Self-esteem is also strengthened and self-confidence increases.

ADULT DIGITAL EDUCATION – FORMAL OR INFORMAL?

When considering the term 'adult education', two meanings of this education can be mentioned. On the one hand, it is the totality of learning processes – formal and informal ones, which complement or extend the education acquired at school. On the other hand, it is practical education in the broadest sense, which allows adults to develop their skills, acquire knowledge, improve their professional qualifications or enrich their personal lives.

In each of the three partner countries, 'adult education' refers to a range of activities aimed at cultural enrichment, professional mobility and extending professional qualifications. These activities may be organised by the school in cooperation with local communities, also involving the labour market and social partners at a territorial level; they may be used to extend or integrate the education provided during compulsory schooling or to replace compulsory education for early school leavers. These activities may simply aim to enrich personal culture to provide or lead to an academic degree.

Formal education is understood as education in the school system, provided by various public and non-public school and educational institutions authorised to teach. Such education follows approved curricula and is based on the standards adopted in the educational system approved by the applicable national regulations. It leads to a qualification confirmed with a certificate, attestation, or a diploma. Informal education is self-directed learning with the aim to acquire knowledge or improve skills, which takes place outside the organised forms of school and extracurricular education and should take place without the participation of a teacher. Another type of education that can be distinguished is non-formal education. These are organised learning activities that do not correspond to the definition of school education. A feature of non-formal education is that it fails to bring about a change in the level of education, but leads to the acquisition and broadening of skills in various areas of professional, social or cultural life. Unlike informal education, non-formal education should take place with a lecturer, instructor or teacher.

The vast majority of adults choose non-formal education institutions and forms of learning if they wish to broaden their knowledge, acquire new skills or

competences. They participate in various types of courses and trainings on their own initiative or are compelled by changes in the labour market, and this form of education helps them to retrain, develop or adapt in a given profession.

In various countries, state institutions have recognised the problem regarding the level of adults' digital skills and are issuing documents to help deal with the high percentage of low-skilled people. Italy is an example here where a national strategic plan on adult ICT competences for 2020 was announced. The plan aims at improving coordination between different entities and processes related to lifelong learning in order to jointly establish national training strategies for the period 2020-2022 to ensure integration and re-entry into the labour market. Italy ranks 25th out of 28 EU Member States in the European Commission's Digital Economy and Society 2020 Index. The level of digital skills varies considerably among those employed in different economic activities. Digital skills are more prevalent in the service sector, followed by public administration, and least prevalent in the industrial and primary sectors. This can inhibit innovation and inclusion in society and the labour market.

FUNDING OF ADULT EDUCATION

Three sources of funding for all forms of adult education can be distinguished, the first one being the funds coming from the state budget which are distributed by various state institutions. For example, in Poland, the institutions involved in non-formal education include the National Training Fund, which allows for the co-financing of the education of employees and employers in various training organisations – both state and private ones. The aim of this fund is to prevent employees from losing their jobs due to competences that are inadequate to the requirements of a dynamically changing economy.

Financial support from the European Commission, which makes funds available for various projects and activities of the organisation, is another source of funding. Financial support in the field of education and training can be obtained, among others, from the ERASMUS+ programme. This is a funding programme that supports activities in the fields of education, training, youth and sport. The European Commission is responsible for the programme's strategies and overseeing its implementation. It is from the ERASMUS+ programme that the 'iAware' project is implemented. The European Social Fund constitutes another example of such a programme, through which the European Union supports the socio-economic development of all member states, and its resources are invested in people, particularly those who are struggling to find work.

A third source of funding for training comprises the trainees' or employers' own financial resources.

ARE ADULTS READY TO IMPROVE THEIR SKILLS?

As the results of the Adult Educational Survey (Eurostat, 2016) show, on average in the European Union, 47.2% of adults aged 25-64 in the year preceding the survey were engaged in formal and non-formal work-related learning. Countries such as Austria, the Netherlands, and Sweden, where at least 60% of adults were engaged in learning, ranked above the average. Certain features of adult education are common to all European Union countries. Younger people are more willing to be educated, and as people get older, their participation in various forms of education decreases. A relationship can also be found between the initial level of education and the willingness to develop one's skills. Those with a higher level of education are more likely to participate in various courses and training.

Increasing ICT skills consists in learning about and benefiting from new technological opportunities. Digital qualifications mean gaining direct experience with tools, machines or software. It is also a theoretical understanding of how new technologies can be used in personal and professional life. The benefits of improving one's skills are both for the individual people and the socio-economic environment in which they operate. From an individual's perspective, enhancing one's skills is an investment in personal development, but also in increasing one's value in the labour market.

Adults learn differently from younger people. They often make educational decisions based on previous experience, therefore the knowledge and skills they seek to acquire must be translated into later practical application. Factors that motivate adults to participate in training and courses include the desire to improve their professional competences, which may be aimed at obtaining a promotion or improving their earnings, the desire to improve their skills, the unwillingness to lag behind developing technologies and the need to operate various digital tools to participate in social and cultural life. The reasons that discourage people from taking up development opportunities comprise a lack of time, insufficient financial resources and a lack of confidence in participating in courses and trainings as well as a lack of knowledge of what is on offer on the learning market, making it impossible to plan appropriate activities.

THE MOST POPULAR AND SUCCESSFUL DIGITAL LEARNING INITIATIVES IN THE 'IAWARE' PROJECT PARTNER COUNTRIES

THE DIGINV PROJECT – Italy

The project develops the Digital Invasion methodology, which was designed in Italy. The methodology improves the digital and communication skills of cultural operators, helping them to become promoters and involve citizens in valorising cultural heritage. It also works to improve the digital skills of the citizens involved (from the youngest to the elderly) by using new technologies to promote cultural sites of interest. Two different outcomes are expected. On the one hand, the digital invasions themselves will allow participants to learn basic concepts of digital communication, reducing digital literacy gaps among participants. The digital invasions will apply the principles of digitisation of production systems, digital storytelling and online marketing to promote cultural heritage to make it more accessible and competitive locally and internationally, enhancing tangible and intangible cultural heritage and participant development in a whole new way. Digital invasions are owners of good practices and the strategic know-how necessary for their transfer to operators and abroad. On the other hand, operators and partner organisations will gain new tools to engage communities in cultural heritage enrichment, as well as to consolidate dialogue with local authorities. This dialogue will strengthen the common line of action at the European level that will be defined in order to involve citizens in the promotion of cultural heritage.

https://www.digitalinvasions.eu/?fbclid=IwAR1qEjgEMGxhuQ0_eFXWJORG855kmlATQL6DycyJo7WkorF_lizPvTW2KRQ

LA SCUOLA CON ME (The school with me) – Italy

The project starts in La Spezia (Italy) at the local Centre for Adult Education (Italian CPIA). The final result is presented on a website in continuous development, which contains materials available free of charge to anyone who wants to teach or learn Italian as a foreign or second language. The blog collects readings, videos, songs, links to many tools and activities: exercises divided by

level, online dictionaries, a verb conjugator and much more. From an educational point of view, we can get more attention through the audiovisual method and more involvement from the students, as they can really work together on the same activity. From an economic and ecological point of view, we can save on photocopies and paper in general. What is more, after lessons, students can practise when and where they choose, following the teacher's suggestions or simply their own interests and working on any device, including a smartphone. In addition, there is the possibility to leave a comment on the blog or to follow their activities through the recently created Facebook page.

http://lascuolaconme.altervista.org

https://epale.ec.europa.eu/en/content/la-scuola-con-me-site-teaching-and-learning-italian

IDEAL – Integrating Digital Education in Adult Literacy – Italy

The main overall objective of the IDEAL project was to provide guidance and training for teachers of adults across Europe in the use of ICT tools and digital methods to better teach basic skills. This was done through an integrated approach to collecting, sharing and disseminating innovative and inclusive teaching and learning practices using ICT tools and digital methods. The project included three types of main activities: the development of four intellectual outputs to provide guidance and training for adult educators and to share the existing educational know-how of the partner organisations; the organisation of two 5-day educational workshops in Finland and Italy; and the organisation of two dissemination events in Finland and Italy. During and after the project, the project team jointly and all partners individually carried out communication and dissemination activities. They also established an effective quality and evaluation system to ensure proper monitoring and evaluation of the project management and results. The intellectual outputs developed under the project include an online toolkit with context and needs analysis, good practice guidelines and video tutorials. All intellectual outputs are available online at www.erasmusideal.com and will be integrated into the curricula of the partner organisations. https://www.erasmusideal.com

INTERACTIVE POOL OF TOOLS for enhancing basic skills and key competences of adults – Italy

The idea for the project originated from an analysis of the situation in the area of adult basic skills proficiency. The OECD Survey of Adult Skills (2013/14) supported by the Commission's DG Education and Culture highlighted that 20% of the EU working-age population had low literacy and numeracy skills and 25% of adults lacked the ability to use ICT effectively. These figures had direct implications for the Europe 2020 strategy, both at an overall and country level, and demonstrated the need to strengthen the skills dimension of the Europe 2020 strategy. Against this background, the main objective of the project was to raise the level of proficiency in basic skills among low-educated adults from Romania, Poland, Germany, Spain and Italy through the following operational objectives: to collect, analyse and categorise existing OER tools and good practices to support the education of low-skilled adults, to develop an Interactive Pool (online database) of tools allowing the categorisation and evaluation of existing tools and the addition of new ones, to develop a Guide to IPool providing step-by-step instructions for using the pool, and to disseminate the results to ensure their use also in other EU countries and other educational fields.

http://www.i-pool.eu

UPSKILL – Portugal

This is a vocational retraining programme in digital technologies that targets unemployed or part-time workers. The programme provides intensive training in tertiary institutions followed by integration into the labour market. The programme was the result of various institutions coming together to organise a national project in response to the growing demand for skilled workers in the ICT sector. Since the start of the programme in March 2020, there has been an increase in companies joining the initiative. The increase in the number of companies is a necessary factor to increase training activities. The programme includes a comprehensive approach to the labour market. It starts with registering companies and identifying the number of professionals they intend to hire by technology and location. The next step is to identify the technological areas, structure the training courses and determine the relevant training content by involving higher education institutions in close cooperation with the companies. The courses last approximately six months, followed by three months of on-the-job training in the participating companies. The project aims to secure employment for at least 80% of the trainees.

https://upskill.pt

PORTUGESE CITIZEN SPOTS - PORTUGALIA

The project has created more than half a thousand points of access to a range of digital services from various public institutions spread throughout Portugal (including abroad) with the help of a trained person. Services provided include, e.g., civil status documents, tax and treasury matters, social security and other public services. All spots are equipped with a two-screen system - one for the citizen, one for the employee - so that citizens can constantly follow the steps taken by the employee, enabling them to learn so that they can then use digital public services themselves. By helping those with low digital skills, the project allows Portuguese citizens to take full advantage of online public services, strengthening confidence in the use of ICT and encouraging all citizens to use it.

E-MOCNI (E-EMPOWERED) – DIGITAL SKILLS, REAL BENEFITS – Poland

Funding for the project came from the European Regional Development Fund under the Digital Poland Operational Programme. The project was implemented by several institutions from the NGO sector in 2016-2019. The aim of the project was to provide ICT training for people who had not yet taken advantage of the opportunities offered by modern technologies, including people with disabilities. This included on-site and online training and provided project participants with an opportunity to learn how to use technology on a daily basis and how to use it to take care of their health, finances or education, professional development, relationships with loved ones or hobbies. As part of this project, almost 18,000 people from 125 municipalities across Poland took part in training courses. Participants were offered more than 100 training topics grouped into different thematic areas, e.g. handling an e-account in the area of Finances, cultural activities on the Internet in the area of Hobbies, social networking on the basis of Facebook in the area of Relations with relatives.

https://e-mocni.org.pl

E-OBYWATEL (E-CITIZEN) NEW DIGITAL SKILLS – Poland

The project involved almost 9,000 people from all over Poland and included three types of training related to the acquisition or development of digital competences. These were traditional training courses aimed at the acquisition and improvement of digital skills in the area of computer operation and the use of computers in everyday and professional life, supplemented by individual classes

aimed at groups with specific educational needs (e.g. people with disabilities). The second type involved online training, which complemented or developed digital skills in specific areas of daily life, and the third type was devoted to blended learning training, which aimed to improve specific digital skills.

https://eobywatel.kig.pl

JA W INTERNECIE (ME IN THE INTERNET)- Poland

This is a funding programme for free training to improve the digital competences of adults so that they make greater use of e-services. Under this programme, almost 15,000 participants took part in training courses in various thematic areas: Parent online, My finances and transactions online, Farmer online, Culture online, My business online. Emphasis was placed on participants' ability to obtain and verify information, communicate using various tools, solve problems, operate software, use public services and e-services. The programme equipped participants with knowledge and tools that developed their competences to function efficiently and safely in the digital world.

https://jawinternecie.edu.pl

CHAPTER 3

-

METHODS AND TOOLS DEVELOPED AS PART OF THE 'IAWARE' PROJECT

The ‘iAware’ project has resulted in twenty 90-minute lesson plans divided into five thematic modules. Experts aimed to prepare effective lessons taking into account the factors that determine the specificity of adult education, which is definitely different from the education of children or young people. The trainer engaged for this type of training should be familiar with the principles of adult education as well as know how to apply them in practice, which will certainly facilitate the achievement of the intended effects and the effective realisation of training objectives.

In the process of adult education, it is essential to ensure that the right conditions are in place to promote the effectiveness of the learning process. They must be comfortable and safe for the learner, as this is one of the motivating factors for undertaking education. Adults often reach decisions based on previous experiences, therefore the knowledge and skills they want to acquire must be translated into later practical applications.

The most fundamental principle in adult learning is the fact that they learn through experience. Each participant comes to the training with his or her own baggage of knowledge, ways of doing things, opinions and beliefs to which they can refer in specific situations. For this reason, when planning the lessons of the 'iAware' modules, the experts moved away from 'traditional' ways of teaching, where the educational process on the trainer's part consisted of delivering extensive theoretical knowledge and the audience's task was to listen patiently. All lesson plans are based on methods and tools that strongly emphasise learner activity and involvement, combining theory and practice, and teaching the use of theoretical knowledge in solving specific, practical problems. The focus is on the learner and their process of acquiring knowledge and skills. The trainer in this approach seeks to create opportunities for new experiences and experimentation.

TEACHING METHODS

A teaching method can be understood as a deliberately and systematically applied way of cooperation between the teacher and the learners, which enables the learners to master knowledge together with the ability to use it in practice. It is the way the teacher-trainer works with the learners. The classification of teaching methods is not standardised. There are many different divisions of teaching methods, and they depend on the division criteria adopted. If we take the activity of the participant as the criterion for division, we can distinguish between administering and activating methods.

Expository methods include those in which the trainer-lecturer is the source of the knowledge. They ensure that the person who teaches is active, while the trainees are the recipients of the content conveyed. They primarily serve the purpose of presenting issues that are new and can be learnt mainly through verbal transmission of content. The learner's activity is oriented towards receiving the message, understanding it and remembering it. The effectiveness of these methods depends primarily on the knowledge, pedagogical skills, and personality of the teacher as well as the organisational and technical conditions in which teaching takes place. Among the expository methods we find, e.g., a lecture, story, description, demonstration, and an instruction.

Activation methods are a group of teaching methods characterised by the fact that in the learning process the activity of the participants in the teaching-learning activities exceeds the activity of the trainer. The group of activating methods includes those in which the teaching-learning process creates conditions for active participation of learners in educational activities. These methods include a problem lecture, discussion method, brainstorming method, situational method, chat, staging or a project method.

Activation methods, in which more senses are involved, allow skills to be fully formed. Knowledge and skills mastered in action are durable and easily adopted in other areas of human activity. Mental activity and cognitive activity are two types of activity are related to the cognitive process. Mental activity can be stimulated by triggering desired mental operations, e.g. by creating a problem

situation. Cognitive activity, on the other hand, can be induced by practical solutions to situations related to everyday life or work practice.

In adult education, the selection of an appropriate method is essential, as on a regular basis learners have already had many experiences and can critically evaluate poorly chosen methods.

ACTIVATION METHODS TO SUPPORT ADULT EDUCATION IN THE 'IAWARE' PROJECT

The activation methods used in the 'iAware' programme allow for maximum involvement of course participants in the learning process. They also help to achieve the learning objectives. However, the main task of the activation methods is to put the learners in a situation in which they feel the need to take the action that the trainer expects of them.

A lecture is one of the most traditional teaching methods. However, relying solely on this method can result in boredom and lack of engagement on the part of the audience. It is a means of helping to familiarise learners with information, to broaden their knowledge, but without elements of activation on their part, it can have a poor effect on learning outcomes. Therefore, instead of a traditional lecture, in many cases a guiding technique has been used, which consists of preparing a series of questions to determine what learners already know about the topic under discussion.

What is more, the chat method has been used, i.e. a trainer-led conversation with participants, during which the trainer helps learners find their way to the right solution to a given problem through preparatory, guiding or collecting questions. The chat is often an introductory chat, which the trainer uses to introduce the audience to the subject of the class and to prepare them for their work. The aim of such a talk is to organise the group for the new work, i.e. to establish the topic and the aim of the class and to pose the question for the training group to work with. Another objective is to provoke mental activity in all the listeners and to develop the need to search for answers on their own. The talk enables new knowledge to be acquired, hitherto unknown relationships between things and phenomena to be established and conclusions to be drawn.

The 'brainstorming' method is yet another teaching method used during the lessons. It provides an opportunity for all, even the most adventurous, ideas for solving a problem to be proposed spontaneously without preliminary verification. Ideas are proposed by all participants in the learning group. Brainstorming takes place in two stages. The first involves gathering ideas, formulating problems and recording them (e.g. writing them on the board), and the second stage focuses on evaluating the ideas and proposals. However, the brainstorming method should follow certain rules. The most important of these is to ensure that learners have full freedom of expression. Each of them has the right to put forward an idea and others can add to it, but all ideas should be beyond commenting, criticising or justifying them.

Discussion constitutes another teaching method that can be found in the lesson plans of the iAware project. This is a teaching method that involves an exchange of ideas between learners, whether the issues expressed are their own views or refer to the opinions of others. In a discussion, the topic must be well formulated: not too difficult or too easy. At the end of the discussion, there should be a summary, providing a brief overview of the results and how the discussion was conducted.

The case study method can also be found in lesson plans. The main advantage of this method is that it allows the trainer to translate theory into a concrete case. It is a detailed analysis that presents a specific issue. The method involves analysing a real or hypothetical case where the trainer presents the trainees with a task to perform and gives useful action tips. The learners exchange their own proposals for solving the problem. Case studies can be complex and include many action steps, but in the case of the 'iAware' project, relatively simple case studies have been used which do not take up much class time and are not very complicated to execute.

The project method also uses the principle of self-study. It is based on practical action concerning the realisation of a certain event. The aim of this method is to search for, organise and systematise information from various sources and then present the results of the work.

In addition, teaching through didactic games is an interesting teaching method that has been developed in the project. Am educational game is a teaching method that uses games as a form of facilitating the acquisition of knowledge and skills. Games are attached to the lesson plans as a teaching aid and comprise games in the form of various interactive quizzes. They can be used to summarise or revise the knowledge gathered in the lessons.

The advantages of activation methods in adult learning include:

- *Making learning activities more attractive,*
- *Enabling learners to speak up, share their experiences, draw conclusions on their own*
- *Ensuring the durability of knowledge acquired in an active way*
- *Integrating learners in the training group*
- *Fostering learner involvement and interest in the topic*
- *Integrating knowledge from different areas of life*

TEACHING TOOLS – MULTIMEDIA MATERIALS AND THE 'IAWARE' PLATFORM

The most important task of the project that we implemented consisted in the creation of the 'iAware' Modular Digital Competence Training Programme. The main objective of this programme was to develop awareness in the use of modern technologies and – by modern technologies – we mean the introduction of new solutions to life as well as technological solutions that require the use of the Internet or electronic equipment – computers, tablets or smartphones.

In addition to the lesson plans themselves, the project also developed an interactive learning environment. For each lesson plan, at least two multimedia materials were developed in the form of a quiz, presentation or an interactive game to enhance the attractiveness of the training and improve learner involvement. These materials also form a self-evaluation element that helps to summarise and check the learners' knowledge on their own. Given the target group, i.e. people with low ICT skills, the quizzes were prepared in a simple form, so that their use was uncomplicated and intuitive for the user.

The project authors decided to use the possibilities of the Internet, considering it an excellent tool to complement and support traditional education. In addition to the 'iAware' programme and its complementary learning environment, the project also resulted in the creation of a learning platform. The entire course, which is divided into five modules according to the training programme, was uploaded to this platform:

1. *Types and identification of online risks*
2. *Counteracting and minimising risks and ensuring online safety*
3. *Active participation in the information society*
4. *Making an informed use of information and communication technology*
5. *Internet trends, active building of a global community and e-citizens.*

The aim of creating the platform was, on the one hand, to increase the attractiveness of the training provided according to the programme developed in the project and, on the other hand, to provide wider access to the project products and to reach a larger target group, also involving learners who have difficulties in attending traditional training, often due to geographical or time barriers or disabilities. Sharing learning materials online can also encourage self-learning and individualisation of the learning process – each learner can return to these materials at any time, any place and at their own pace of learning.

The platform was developed by the Italian project partner PRISM and is available at https://www.iaware-education.eu. In the materials section, you can find all the results developed within the project, divided into two categories: for the learner and for the trainer. It is available in four language versions – English, Polish, Portuguese and Italian. A module related to user registration on the platform is available for learners who are interested. The website has been specially designed to be easy to read so that all learners, even those with the lowest level of internet skills, can find the right information.

The assumption accompanying the experts preparing the programme was to focus on the implementation of practical exercises. The examples prepared were based on standards functioning in daily, social or professional life and are intended to relate to the learners' experience. The experts prepared a set of materials for the learners covering all five modules. In addition to the interactive materials developed by them, the course includes links to other websites, videos with similar content and other examples. In this way, after the course, learners will be able to refine the knowledge and skills acquired in the course on their own. A detailed discussion of the lesson plans and the accompanying materials can be found in the next section related to the programme, which comprises the programme itself, materials and guidelines for trainers who wish to work with the 'iAware' method.

CHAPTER 4

-

THE 'IAWARE' PROGRAMME

PROGRAMME ASSUMPTIONS, OBJECTIVES AND RESULTS

The project 'iAware – Innovative Programme for Adult Education' is implemented by a partnership of three organisations from Poland, Italy and Portugal. The Polish organisation EURO-FORUM is its leader, while the Portuguese COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL and the Italian PRISM – PROMOZIONE INTERNAZIONALE SICILIA – MONDO are the partner organisations. The project is a response to the jointly diagnosed problem of insufficient digital competences of adults. It results from the lack of modern educational programmes that would include content that goes beyond learning the skills of standard operation of modern devices and use of network resources. Thus, the project addresses contemporary challenges related to the development of technology and the Internet, and meets the need for adults' continuous improvement of ICT competences in the current Internet reality.

The main objectives of the project comprise:

- *creation of a state-of-the-art ICT education programme for adults taking into account contemporary challenges in the field of Internet security and informed use of online resources;*
- *provision of the right educational content, tools, knowledge and skills to develop among adults attitudes of conscious use of modern technologies to ICT trainers and educators of adults;*
- *improvement of key competences in ICT among adults in the European Union and building of an informed information society.*

As part of the project, the following results have been produced:

1. The 'iAware' Modular Digital Competence Training Programme

This is an innovative training programme to develop digital competences among adults. Developed in a practical and functional way, it has been divided into five thematic modules addressing issues related to online threats, their identification, prevention, active participation in the information society or conscious use of modern information and communication technologies. The training programme is accompanied by an elaborate educational supplement containing the content appearing in the programme in the form of multimedia – quizzes and video material.

2. The "iAware" learning platform is available at https://www.iaware-education.eu .

This is a web-based application where all the materials developed as part of the project – the programme, the educational supplement and this e-book – are made available in a digitised form. This will enable trainers to deliver training in a more attractive way, using multimedia dedicated to individual modules. The platform will be available to all adults wishing to improve their competences in the conscious use of modern digital technologies.

3. A methodological guide with instructions for trainers, i.e. this e-book

This is an instruction manual on the use of tools for ICT trainers and educators working with adults published in the form of an e-book, which focuses on substantive support for trainers' development in the competence areas most in need of intervention, in relation to the needs diagnosed in the project. All content included in the e-book is as universal as possible, i.e. it can be implemented in both the partnership and other European countries.

PROGRAMME STRUCTURE

All activities in the project are designed to contribute to the ultimate goal, in line with the policy of the European Commission, of improving the key competences of ICT in adults in the European Union and building the information society. This will be achieved through the creation of a modern digital competence education programme for adults, which will take into account the contemporary challenges of the Internet, including an understanding of both the risks and opportunities of web development.

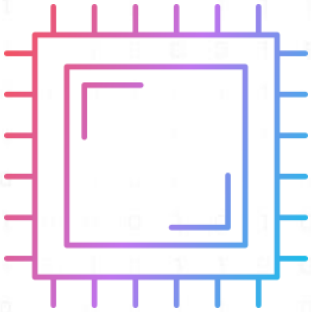
The entire programme was divided into five modules. Each module consists of four 90-minute lessons, as shown in the diagram:

Module 1	Module 2	Module 3	Module 4	Module 5
Lesson 1	Lesson 1	Lesson 1	Lesson 1	Lesson 1
Lesson 2	Lesson 2	Lesson 2	Lesson 2	Lesson 2
Lesson 3	Lesson 3	Lesson 3	Lesson 3	Lesson 3
Lesson 4	Lesson 4	Lesson 4	Lesson 4	Lesson 4

In total, the programme contains twenty lesson plans that are complemented by multimedia teaching materials. Both the lesson plans and multimedia for the course participants complement each other. All the materials have been made available in digital form on the iAware platform at: https://www.iaware-education.eu.

The individual modules cover topics such as:

- *Module 1 – Types and identification of online threats*
- *Module 2 – Counteracting and minimising risks and ensuring online security*
- *Module 3 – Active participation in the information society*
- *Module 4 – Conscious use of ICT skills*
- *Module 5 – Internet trends, active building of a global community of e-citizens*



MODULE 1
-
TYPES AND IDENTIFICATION OF ONLINE THREATS

The Internet is an essential medium without which it would be difficult to imagine functioning effectively in the modern world. Yet, it is a well known fact that using the web can pose quite a threat to its users. When used properly, the Internet can serve both the user and society. However, it is mainly up to the rationality of the users to make proper use of the possibilities of the web. The user is the weakest link in the chain, which is why the experts decided to equip the 'iAware' programme participants with knowledge on how to use the Internet sensibly. The first module of the 'iAware' programme covers the different types and identification of online threats.

It provides for the following topics:

1. *Spam and scam*
2. *Phishing*
3. *Online privacy*
4. *Digital footprint*

Very similar topics will be discussed in module two - 'Counteracting and minimising threats and ensuring online security', which will constitute a further development of the topics from module one. The lesson plans in module one focus on presenting, defining and identifying the threats. Lessons in module two will show how to effectively defend against the threats in question.

Lesson 1

-

Spam and scam

The main objective of the first lesson is to identify the threats of spam and scam and to understand what possible risks they pose. They are both fairly common phenomena and the trainees may have already encountered them. When identifying these phenomena, the trainer should determine the level of learners' knowledge of them and refer to their previous experiences. Learners should be allowed to attempt to identify the threats themselves and possibly supplement their knowledge. Spam, for example, can be defined as unsolicited messages sent electronically via e-mail or various instant messengers whereas Spam is usually sent in bulk, most frequently in the form of various advertisements. The essence of this type of message is to send a large amount of information with the same content to a very wide audience. In other words, spam can be defined as the sending of unexpected electronic messages on a mass scale in an anonymous manner.

When considering the issue of spam, the definition of bulk e-mail is also important to consider. Basically, two categories of bulk e-mail can be distinguished. The first category constitutes unsolicited commercial offers, otherwise known as commercial spam of an advertising nature, which is prohibited under European law. The second group of bulk e-mail comprises unsolicited bulk e-mail. This category includes e-mails of a usually non-commercial nature, e.g. appeals from social organisations, charities, requests for help, or mass warnings.

In order for a message to qualify as spam, the following three conditions must be met:

- *the message content is independent of the identity of the addressee.*
- *the message recipient has not given his or her prior consent to receive the message*
- *the message content gives rise to an expectation that the sender will derive a disproportionate benefit from the sending of the message.*

Trainers should remind the learners that, although it appears to be a relatively harmless phenomenon, spam generates a number of problems and it is a nuisance to recipients. It clutters Internet users' inboxes, blocks the Internet, overloads servers and takes up disk space. What is more, it poses a threat to the security of Internet users, as it is a source of viruses. Despite numerous safeguards, spam e-mails arrive in large numbers. Their senders often use unethical ways to send spam, e.g. by impersonating a bank or other trusted institutions. They may also 'cleverly' title messages in such a way that they are very likely to be read by intrigued Internet users. An email with the title "you have received an inheritance" or "you have won a prize" may effectively encourage the recipient to read the content of such an unsolicited message.

Learners should be made aware that sending unsolicited messages is regulated at EU level as well as in each Member State. One of the tasks during the class is to find out which country's laws regulate these phenomena. Trainers should therefore check before class which laws or regulations regulate spam and scam in their country.

MODULE	Types and identification of threats in the Internet	LESSON UNIT	1	TOPIC	Spam & scam

LEARNING OUTCOMES:

- Learners will be able to name threats such as spam and scam.
- Learners will be able to identify spam or scam.
- Learners will understand the possible dangers of these activities.

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY (time: 15 mins)	To acquaint learners with the goals and results of the training To familiarise learners with examples of scam and spam messages	1. The trainer greets the learners 2. The trainer defines and presents the aims of the lesson to the learners: • After today's lesson you will know what spam and scam are • You will understand how spam works • You will know why it is not worth answering e-mails that are spam 3. The trainer acquaints the learners with the lesson plan and its successive stages 4. The trainer asks the learners to open their e-mail (if they have one). S/he asks them to find among the messages in the e-mail, examples of messages	• a set of suspicious messages in an electronic form • a projector and computer with internet access for the trainer • work with computers- learners have access to a computer with the Internet connection

		sent to them without their knowledge, which they did not want and which they deem unnecessary. 5. The learners search their e-mail, share the "most interesting" messages on the group forum. The trainer highlights the different types of these messages.	
Task **TRY TO NAME** (time: 15 mins)	To name the phenomenon of spam To define scam in connection with spam	1. The phenomenon of SPAM for e-mail users is quite well-known; therefore, depending on the learners' knowledge, the trainer may ask them to define spam themselves or s/he provides a definition and shows examples in an e-mail account. Exemplary definitions of SPAM in such general terms can be found in the chapter on this lesson in the e-book. 2.The trainer points out to the learners that spam usually goes hand in hand with another phenomenon, i.e. scam. The trainer explains that scam can be translated as a sham/ swindle because it is a scam where first trust is gained and then used, for example, to extort money. A typical activity is sending mass correspondence (spam) electronically and offering the victim, in such a message, a share of huge profits in return for an alleged intermediation requiring little investment.	• a projector and computer with internet access for the trainer • work with computers - learners have access to a computer with the Internet connection

Task **ACT** (time: 25 mins)	To familiarise the learners with one type of a scam	1. The trainer introduces the learners to the remaining activities of the lesson. Based on the previous lesson stage, the trainer describes one of the most famous types of scam. 2. Perhaps the most famous example of spam is the so-called "Nigerian scam", a scam which consists in extorting funds and personal data sent voluntarily by victims directly to the fraudsters. Various types of stories (e.g. about acquiring an inheritance) are sent as spam to e-mail accounts. The fraudster usually offers the victim to split a large amount of money under different conditions, but only after making a money transfer to his account. In fact, money sent by the victim is intercepted by the fraudster. 3. The trainer points out that SPAM and SCAM are very serious things that happen online, but sometimes they can be treated humorously. 4. The trainer sends learners a link to the video on YouTube or plays the video on the screen. 5. The trainer talks to the learners about spam, if they have ever received such an e-mail in their inbox, what they did in such a case and discusses what consequences of responding to spam like in the example video could be.	• a projector and computer with internet access for the trainer • work with computers- learners have access to a computer with the Internet connection As a fun fact: The Ig Nobel Prizes are humorous equivalents of the Nobel Prizes for works that seem fun and for discoveries that cannot or should not be repeated. In 2005, such a collective literary award went to "entrepreneurial Nigerian writers" for creating and using an email with characters, each of whom needed some money to recoup a huge fortune that they would gladly share. • Link to the video "This is what happens when you reply to spam" (10 min) https://www.youtube.com/watch?v=_QdPW8JrYzQ

		6. The learners answer the trainer's questions and share their reflections on the watched video.	• If anyone is interested, they can watch the next part entitled "More adventures in replying to spam" (10 min) https://www.youtube.com/watch?v=C4Uc-cztsJo
Task **ACT** (time: 20 mins)	To understand how spam works and what its consequences may be To present an overview of the different types of spam To define other terms related to spam	1. The trainer explains to the learners that it is estimated that about 80% of all daily messages are unwanted mail, i.e. spam. 2. The trainer asks the learners to think about the consequences of sending so many messages. Learners may be divided into smaller groups so that they think about the question, and then present the results of their work on the forum and compare them with the effects of the work of other groups. Learners can check their e-mail boxes. Examples of consequences that can be mentioned: •Locking disk space •Threat of infection by a harmful virus •Slowing down servers as a result of increased spam processing work •Possibility to lose received messages by blocking the inbox •Creating a chaos in one's inbox, which may lead to a loss of important messages	• a projector and computer with internet access for the trainer • work with computers- learners have access to a computer with the Internet connection

- Problems while reading regular mail
- Phishing of contact details
- Reduced confidence in internet advertising
- Transmission of undesirable content by the user (e.g. content for adults, offensive)

3. The learners' next task will be to classify and divide spam messages into categories.

- Ads
- Inheritance
- Fictitious e-mails- here the trainer should invite learners to the next lesson, entirely devoted to the phenomenon of data extortion and phishing

4. The trainer asks the learners to consider whether they have encountered spam somewhere outside of the e-mail. Perhaps they get unwanted phone calls or traditional letters with advertising mail that they didn't order. This can also be called spam. The learners share their experiences with the group. This task, depending on the size of the training group, can be performed with the entire group or divided into teams of several people.

5. The trainer explains to the learners that the person who sends spam, i.e. the unsolicited messages, is called a spammer.

		6. On the other hand, to send out such messages, special software is used, specially designed to spread spam and called bots or spambots.	
GOOD PRACTICES (time: 10 mins)	The learners together with the trainer create a list of best practices regarding unsolicited e-mail.	1. The learners consider how they can reduce spam and share their comments on the group forum. 2. On the Internet they search for legal regulations concerning spam that are binding in a given country.	• a projector and computer with internet access for the trainer • work with computers- learners have access to a computer with the Internet connection
FEEDBACK/ REFLECTION TASK (time: 5 mins)	To revise and verify the acquired knowledge. To obtain feedback from learners regarding the lesson.	The trainer summarises the lesson and checks the learners' reaction to the lesson (positive / negative).	
Self-study quizzes Extended learning Consolidation	Use another module where you will learn how to prevent phishing and how to detect such fraud - 'Counteracting and minimising threats and ensuring network safety'	The trainer summarises the lesson. If the trainer wishes to continue the lesson on the phenomenon of scam, s/he needs to go to the next lesson in this module dealing with data extortion and phishing. After expanding both topics, the module: *Counteracting and minimizing threats and ensuring network safety* may be visited.	

Two multimedia quizzes are provided for the lesson.

Quiz 1

This quiz can be used at the end of the lesson as a summary of what learners should know after the lesson and can be taken together, e.g. on an interactive whiteboard, or by each learner individually on their computers/tablets. Trainers could also ask the students to do the quiz themselves at home as a self-evaluation. The quiz consists of ten questions to be answered TRUE or FALSE. The content of the quiz with the correct answers is shown below.

- *Spam means sending messages electronically in an anonymous manner. TRUE*
- *Scam is the fraudulent induction of trust in order to defraud. TRUE*
- *Spam can take the form of sending out 'good luck chains'. TRUE*
- *Spam is sent anonymously to make it difficult to detect the actual sender. TRUE*
- *Spam content can also appear on Internet forums.*
- *Spam is a completely harmless phenomenon. FALSE*
- *Social networking sites such as Facebook and Instagram are safe and users are not exposed to spam and scam.*
- *A scam message is a malicious message designed to defraud. TRUE*
- *A scam message may confusingly resemble a message from real public institutions. TRUE*
- *It is safe to click on all links provided in emails. FALSE*

Quiz 2

This quiz is also a summary of the lesson – a compilation of all the key information to be remembered from the lesson. The trainer can display it on the interactive whiteboard at the end of the lesson or learners can display it on their devices. It can also be a very brief reminder of the lesson input before the first

lesson of module two, which discusses effective defence against spam and scams. Below the content of this short summary is presented.

Screen 1

SPAM

Mostly e-mails sent in bulk to many recipients

Recipients did not order or accept to receive such messages

It also occurs in other communication channels - text messages, instant messaging or social networking sites

Screen 2

SPAM

Some of these messages may be harmless: they simply litter the mailbox

There are messages that can pose a threat to the user

The purpose of dangerous messages is to defraud the user's data or money

Screen 3

SCAM

A very common phenomenon on the Internet

A form of online or telephone scam

Based on the induction of trust in order to lead to phishing

Screen 4

SCAM

In cases of online fraud, scammers use forms or fraudulent websites impersonating real sites

Criminals can also impersonate public institutions as well

Popular scams include offers of products at surprisingly low prices, unexpected prizes in competitions, stories of an inheritance received but also support for sick or disabled people

Lesson 2
-
Phishing

It is likely that most mobile phone users and email account holders have received a suspicious message at least once in their lives. If it was accompanied by a link, it was most likely the case of phishing. Unluckily for the average web user, scammers are getting better and better at taking over data and then using the information they gain to deceive their victim. Therefore, the main objectives of this lesson are to make learners aware of the need to protect their data when navigating the web and to identify the phenomenon of phishing.

Examples of definitions of phishing that can be provided to class learners:

- *Phishing is a method of fraud that involves impersonating an institution or person known to the victim in order to trick them into providing valuable information or infecting their devices with malware or persuading the victim to take certain actions.*
- *Phishing is a method of fraud that most commonly involves sending emails or SMS messages claiming to be from reputable companies or public institutions in order to entice people to disclose personal information such as passwords or credit card numbers.*
- *Phishing is a social engineering attack aimed at tricking the victim into voluntarily disclosing confidential information.*
- *Phishing is an online scam in which a third party impersonates a company or institution in order to trick a person into logging in to electronic banking and ordering as well as authorising a payment transaction.*

The term 'social engineering' is also linked to the concept of phishing and seeks to exploit the weakest links in the security chain, namely people – by appealing to vanity, greed, curiosity and altruism or to their respect or fear of authority in order to persuade them to disclose certain information or to gain access to an information system. In other words, social engineering involves deceiving people by persuading them to disclose their private data, such as passwords or bank accounts, or to grant access to a computer in order to discreetly install malware.

MODULE	Types and identification of threats in the Internet	LESSON UNIT	2	TOPIC	Data extortion - phishing

LEARNING OUTCOMES:

- Learners know that they have to protect their data when surfing the web.
- Learners will learn the meaning of the terms data extortion, phishing.
- Learners are aware that Internet fraudsters may be interested in their data.
- Learners will understand that by disclosing their information, they may become a victim of internet fraud.

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY (time: 25 mins)	To acquaint the learners with the lesson aims and results To introduce the learners to the topic of the lesson To determine by the learners the type of data that may be phished in the Internet	1. The trainer greets the learners. 2. The trainer defines the lesson aims and presents them to the learners: •After today's lesson you will know what data extortion is •In today's lesson you will learn the meaning of the word PHISHING •You will familiarise yourselves with the different types of phishing methods 3. The trainer acquaints the learners with the lesson plan and its successive stages 4. The trainer asks the learners to think for a moment what data can be requested from the point of view of the person who would like to use them inappropriately. In order to help	• a set of printed suspicious messages • a set of suspicious messages in an electronic version • a projector and a computer with internet access for the trainer

		guide the learners to the topic, trainer can use examples of phishing messages in a printed or electronic form. Then the trainer asks the question "What data do the senders of such messages want to obtain from us?" 5. Brainstorming with the learners- all ideas connected with data are written on the board. Data that may be of interest to fraudsters include: name and surname, date of birth, PESEL identification number, ID card number, place of residence, telephone number, electronic banking login details, bank account number, login details for online stores or auction platforms, email login details, usernames and passwords for various websites and social networks, photos. 6. The trainer briefly summarises the collected ideas and engages the learners in the next stage - considering what such data can be used for (e.g. extorting a credit, loan, setting up a fake bank account, making various purchases, setting up fake accounts or a profile on a social networking site, impersonating a given person and writing offensive opinions or comments, entering into false contracts, conducting business activities, forging documents, identity theft).	
Task **TRY TO NAME (time: 10 mins)**	To define the terms 'data extortion' and 'phishing'	1. The trainer asks the learners to try to sketch the definition of the term 'data extortion' on their own 2. The trainer combines the concept of data extortion with the concept of PHISHING and gives its definition. Exemplary definitions of the PHISHING phenomenon can be found in the book in the chapter assigned to this lesson.	• a projector and computer with internet access for the trainer •work with computers - learners have access to a computer with

			the Internet connection • To facilitate better and quicker memorisation, the trainer may refer to a YouTube video explaining the concept of phishing. Examples: - *What is phishing?* - *https://www.youtube.com/watch?v=BnmneAjVrM4* - *https://www.youtube.com/watch?v=hG6XJROw8HY* - *https://www.youtube.com/watch?v=BzNh-gxosE8*
Task **ACT (time: 20 mins)**	To understand the mechanisms of phishing To find the "'weakest link' To get to know the concept of 'social engineering'	1. The trainer can divide the learners into groups and send each group a link or give an example of an e-mail printed on a piece of paper that constitutes an example of phishing. With a small number of learners, group work can be replaced with individual work. 2. The trainer asks the learners to look at sample e-mails that were phishing attacks and consider why these attacks are successful. 3. After a short reflection, each group presents their conclusions.	• a projector and computer with internet access for the trainer • work with computers- learners have access to a computer with the Internet connection • Examples of e-mail messages illustrating the

	To present an overview of the different types of phishing	4. The trainer points out that, unlike other online threats, phishing does not require particularly advanced technical knowledge, because criminals do not exploit the technical vulnerability of the device software, but use manipulation techniques called social engineering. It turns out that the weakest link is a person who doesn't exactly check the origin of the email. 5. The trainer emphasises that phishing attacks consist in triggering certain emotions- fear, anger, curiosity, so as to cause an automatic, quick reaction. 6. The trainer introduces the learners to the concept of 'social engineering'. Sample definition to be found in the e-book. 7. An overview of different types of phishing: the trainer points out that the phishing procedure does not only concern e-mail. - Spear phishing - this is a type of attack that targets one institution or person. An attack of this type is profiled, i.e. the attacker collects information about his victim beforehand and only then constructs a message that is to convince the victim to visit a fake website or download a crafted file - E-mail cloning- an attack in which the criminal uses a previously sent real message to the user. The attacker copies the genuine message template and places a link to a malicious website in it	PHISHING phenomenon can be found at: - https://lts.lehigh.edu/phishing/examples - https://www.phishing.org/phishing-examples - https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive

		- Redirection to another page- deliberate redirection of users visiting a certain webpage to another, most often fabricated by the stacker - Text message and phone phishing- this attack uses text and voice messages, where criminals use special tools to impersonate the phone number of a specific company or send fake text messages	
GOOD PRACTICES **(time: 30 mins)**	To exchange the learners' own experiences. To summarise and organise the acquired knowledge	1. The trainer asks the learners if they have had any experiences with phishing, if they were a victim of it, or if they encountered this phenomenon in their immediate environment. 2. The trainer, together with the learners, carries out an exercise that gathers knowledge and summarises the work. 3. The learners work in groups (with a small number of learners it can be done individually) 4. The trainer asks the learners to create their own example of a phishing e-mail. They can use examples of such messages from the previous stages. Learners work in text editors or in their e-mail account. In order to organise the work, the learners should consider addressing the following questions: •What could the purpose of phishing data be? •What data would they like to extort? •Where and how could they use this data? •How to formulate an e-mail to make it credible?	• a computer, a projector, access to the Internet • a text editor or an email account

		5. The learners create their e-mails, present the results of their work, answer the questions posed above and exchange comments with other learners.	
FEEDBACK/ REFLECTION TASK (time: 5 mins)	To revise and verify the acquired knowledge.	The trainer summarises the lesson, encourages the learners to deepen their knowledge on their own and to participate in the lessons of the next module: 'Counteracting and minimising threats and ensuring network safety', in which they will be able to expand the knowledge acquired during this lesson.	
Self-study quizzes **Extended learning** **Consolidation**	Use another module where you will learn how to prevent phishing and how to detect such fraud - 'Counteracting and minimising threats and ensuring network safety'	Use another module where you will learn how to prevent phishing and how to detect such fraud - 'Counteracting and minimising threats and ensuring network safety'	• You can check the links: - https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing - https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf • and the one collecting UNIT1 and UNIT 2 from this module: - https://www.youtube.com/watch?v=NI37JI7KnSc

Phishing can take various forms in each country. Trainers should prepare such examples of Internet scams to which Internet users in the countries concerned are most likely to be exposed.

Two multimedia quizzes are provided for the lesson.

Quiz 1

This quiz can be used at the end of the lesson as a summary of what learners should know after the lesson and can be done together, e.g. on an interactive whiteboard, or individually on their computers/tablets. Trainer could also ask the students to do the quiz themselves at home as a self-evaluation. The quiz consists of ten questions to be answered TRUE or FALSE. The content of the quiz with the correct answers is shown below.

- *Phishing is an attack aimed to defraud data. TRUE*
- *A phishing attack can be based on text messages. TRUE*
- *Instant messaging can also be used for phishing. TRUE*
- *Only public institutions are victims of phishing attacks. FALSE*
- *Phishing attacks are largely based on social engineering methods. TRUE*
- *Anti-virus software protects against phishing. FALSE*
- *People can freely give out their data on the internet. FALSE*
- *Installing applications from a link in a text message is risky. TRUE*
- *Spear-phishing is an attack aimed at a specific recipient. TRUE*
- *Only Windows computers are vulnerable to phishing. FALSE*

QUIZ 2

This quiz is also a summary of the lesson – bringing together all the key information that learners should remember from the lesson. The trainer can display it on the interactive whiteboard at the end of the lesson or alternatively learners can display it on their devices. It can also be a very brief recap before the second lesson of module two, in which learners will learn how to effectively defend themselves against phishing attacks. Below the content of this short summary is presented.

Screen 1

Using antivirus software does not protect against phishing attempts.

Using anti-virus software reduces the risk of your computer being infected by viruses, but does not protect against phishing attacks.

Screen 2

Phishing attempts do not only occur via email.

Phishing can also occur over the phone – when installing applications from unverified sources, through text messages or voice calls.

Screen 3

A trustworthy company may be entered in the email sender field.

Remember that it is easy to change the sender information in the email client profile.

Screen 4

Banks and other trustworthy companies do not ask for personal information in emails.

If you receive such a request, it is best to delete such an email immediately.

Screen 5

All types of files in attachments can be a threat.

It is not only files with an .exe extension that pose a threat and do not open attachments in emails if you do not know their origin.

Screen 6

Be careful when shopping online.

Always buy from companies, shopping platforms or sites that are trusted.

Screen 7

Emails that contain links to other websites can be more dangerous.

Do not click on links if you are unsure of the email sender.

Screen 8

Remember that your data is a valuable commodity.

Do not enter your details such as your name, address, payment card or bank account number on random websites.

Lesson 3

-

Online privacy

The topic of online privacy is an essential and increasingly widely addressed and discussed issue in contemporary digital education. Privacy is the currency of the Internet, and a user's online privacy depends on the ability to control both the amount of information given and access to it. By connecting to the Internet users become part of a huge database, by moving around the web they leave their footprints and by using social media they themselves reveal information from their private lives.

On the internet, it is difficult to protect one's privacy and personal information. Many sites encourage users to share information about themselves, not only their name, but also photos, videos, work information, interests etc. The main aim of this activity is to make students aware that by publishing such information, they are sharing it with the whole world, and that what goes on the Internet stays there forever.

The best way to protect the privacy of Internet users is to educate them. An additional aim of such classes is to make Internet users more and more aware that the Internet is a public place and that they should take care of their privacy there.

When delivering a lesson on privacy, trainers need to adapt to the group of learners they are working with. It is usually the case that the younger the learners are, the more frequently they use more websites, social networks or online shopping platforms and the more easily they give out their data online. Trainers should also note that everyone draws the line a little differently between what is personal and what others can access. Group members may view privacy differently. Some learners may be comfortable posting photos of personal moments on social networks, while others may consider it inappropriate. For some, sharing information about life moments such as a wedding is not unusual, while others do not even wish to give their name. The different approaches of the learners can serve as an ideal starting point for a discussion in the training group. Trainer may include such a point in the lesson plan.

The right to privacy is also addressed in the lesson plan. There is EU legislation on privacy, including the protection of personal data. This includes the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. However, in each country

the right to privacy is regulated by other acts. The aim of the task in the lesson is to find national legislation regulating privacy. Before the class, the trainer should prepare information about privacy protection in the country where the class is held. Trainer can also use various regulations of websites during the class.

MODULE	Types and identification of threats in the Internet	LESSON UNIT	3	TOPIC	What is online privacy?

LEARNING OUTCOMES:

- Learners will understand the concept of the right to privacy
- Learners will become acquainted with various aspects of privacy
- Learners will know what sensitive and personal information means

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY discussion (time: 15 min)	To familiarise learners with the training objectives, discussion on the limits of privacy.	1. The trainer greets the learners. 2. The trainer defines the goals of the lesson and presents them to the learners. After today's lesson you will: • know what privacy is • understand why privacy is a valuable asset • what sensitive data and personal data mean 3. The trainer acquaints the learners with the lesson plan with its successive stages. 4. The trainer asks example questions related to different types of privacy and asks learners to briefly justify their answers. • How do you feel when someone is standing too close? • How do you feel about touching another person without their consent?	• Computer, projector, internet access • Tape or chalk/ markers

		• What do you think when someone spreads rumors about you? • Would you allow strangers to read your e-mail or SMS? • Would you like other people to know what websites you use or what pages you browse on the internet? • Would you like your photos to be distributed without your consent? • Would you mind if your address or phone number was known to everyone, even people you don't trust? • Do you think your health data should be accessible to other people? 5. The trainer summarises the discussion and points out that everyone needs a space around them that belongs only to a given person. Not only does it refer to the physical aspect, but also to various data that we do not want to share with other people.	
Task **TRY TO NAME (time: 10 mins)**	To name terms: Privacy Right to privacy Personal data Sensitive data	1. Referring to the discussion from the previous stage of the lesson, the trainer states that the space that we consider only ours can be called "privacy". 2. Together with the learners, the trainer attempts to distinguish different aspects of privacy. This can be done by drawing the diagram on the whiteboard. 3. The possible division of privacy aspects includes those related to: • physical contact	• Computer, projector, internet access

		• communication- reading e-mails, SMS, eavesdropping on conversations • information about us 4. The trainer explains that everyone has a right to privacy in everyday life. Privacy is protected by law. 5. The trainer explains that there are two more concepts related to privacy: personal data and sensitive data. Personal data can be understood as any information relating to an identified or identifiable person (e.g. name, surname, date of birth). Individual information that, when combined together, may lead to the identification of a given person, is also treated as personal data. Sensitive data is a special type of personal data, the collection and processing of which is secured with stricter rules than the use of other types of data. The sensitive data include, among others, data related with racial or ethnic origin, health, sexuality or sexual orientation, religious or philosophical beliefs.	
Task **ACT** **(time: 20 mins)**	To become familiar with the institutions and legal acts that ensure the right to privacy.	1. The trainer reminds that the right to privacy was mentioned in the previous part of the lesson 2. The trainer asks the participants to find: • legal acts that ensure the right to privacy for everyone • institutions that protect privacy Learners may be divided into groups that look for information on international acts (e.g. the International Covenant on Civil and Political Rights or the European Convention on Human Rights), as	• Computer, projector, internet access • computers for learners

		well as information on legal regulations in individual countries. In the activity, we do not focus on the details of legal acts, but it is important to point here that there are many institutions that care about privacy, and the right to privacy is treated as one of the personal rights and there are a number of legal regulations regarding these issues. 3. The learners discuss all together what they have found on the Internet regarding the protection of privacy.	
Task **ACT** **(time: 25 mins)**	To show a process of collecting users' data and creating users' digital profile	1. The trainer divides the learners into teams of several people. Each team chooses one person from among themselves. On a piece of paper, learners write down some data (7-10) about this person, which have been made available on the Internet (e.g. in a search engine, on Facebook and other social media, inter alia websites visited, music listened to, movies watched, political views, age, or first name and surname, whether s/he commented on various topics somewhere, whether s/he participates in discussions on online forums, or browses advertisements or online stores). After writing down the data on a piece of paper, this piece of paper is passed to the team sitting nearby. 2. After handing over the piece of paper, instruct the teams to play the role of employees of companies dealing with data collection and, on the basis of the information received, to try to describe the person and think about what the data can be used for. Or we can ask what products this person could buy. 3. The teams present the results of their reflections on the forum, and the people to whom these descriptions relate reveal themselves and assess which part of this description is correct.	• Computer, projector, internet access • Sheets of paper, pens

GOOD PRACTICES **(time: 10 mins)**	To understand that privacy boundaries vary from person to person To understand that online privacy is a value	The trainer asks the participants: What is not worth sharing on the Internet? What information is not worth publishing on the web? What information may never be given under any circumstances? 2. The trainer directs the learners to check their profiles on websites with regard to what data they make publicly available and to check the security policies of these websites.	• Computer, projector, internet access
FEEDBACK/ REFLECTION TASK (time: 10 mins)	To revise and verify the acquired knowledge.	The trainer emphasises the special nature of privacy and data in the digital world. Summary of the lesson, a review of concepts related to privacy once again. Answering learners' questions. Encouraging learners to take advantage of the next module on how to protect privacy on the Web.	• Computer, projector, internet access
Self-study quizzes **Extended learning** **Consolidation**	Use another module where you will learn how to prevent phishing and how to detect such fraud - 'Counteracting and minimising threats and ensuring network safety'	For more information on how to prevent loss of privacy in the Internet, see the module: *Counteracting and minimising threats and ensuring network safety*.	

An extension of this lesson, which deals with the issue of privacy, is the following lesson on the digital footprint. Two multimedia quizzes are provided for the lesson.

Quiz 1

The quiz is a summary of the lesson and brings together all the key concepts that have emerged during the lesson. In short sentences, the information that learners should remember from the lesson is suggested. There are several ways of working with the quiz. The first involves displaying it on a screen and doing it together with the group at the end of the class. The second option is for each learner to work with the quiz independently during the lesson. The third option is for the learner to return to the quiz at home, after the lesson is over, as a summary and recap of the lesson. The fourth option entails that the quiz is treated as a memory refresher of the lesson on privacy and a prelude to the next lesson on digital footprint. It is up to the trainer how they want to use this interactive exercise. Below the content of the quiz is presented:

Screen 1

Personal data

- Information about you, thanks to which it is possible to find and recognise you among others
- This includes, e.g. name, address, telephone number, e-mail address
- Personal data is protected by law

Screen 2

Processing of personal data

- This is the performance of operations on personal data by automatic or manual means
- It is, e.g. activities such as collecting, organising, arranging, storing, viewing, disseminating, deleting and destroying
- There are rules of law that govern the processing of personal data

Screen 3

Privacy

- The ability to keep information and data about oneself private
- The right to privacy is regulated by various acts of law
- Your privacy online depends largely on how much information you provide about yourself

Screen 4

Digital footprint

- This is information about a particular person's online activities
- It is made up of, among others, photos, posts on forums, blogs, social media, information about the websites you visit, but also your IP address, information about your system or the browser you use
- Every internet user has a digital footprint

Screen 5

Profiling

- A mechanism used to categorise internet users according to characteristics, behaviour, and preferences
- It can be observed, e.g., in presenting advertisements that are best suited to the needs of a particular person
- In addition to commercial purposes, the profiling mechanism can be used by state authorities to enhance security.

Quiz 2

The quiz consists of ten questions which learners assess as TRUE or FALSE by ticking the appropriate boxes on the screen. The content of the quiz with the correct answers is shown below. The quiz can be used at the end of the lesson as a summary of what learners should know afterwards, and can be done together, e.g. on an interactive whiteboard, or by each learner individually on their computers/tablets. Alternatively, learners can be asked to take the quiz themselves at home as a self-evaluation.

- *There is no anonymity on the internet. TRUTH*
- *The data we use every day can be used to cause harm in the wrong hands. TRUE*
- *Everyone who uses the internet has a right to privacy TRUE*
- *There are legal acts that protect privacy. TRUE*
- *My privacy online is also protected by law. TRUE*
- *It is very easy to protect your privacy and personal data on the Internet. FALSE*
- *You should publish information about yourself carefully. TRUE*
- *We leave a lot of traces on the Internet, also not fully consciously. TRUE*
- *Personal information is limited to such data as name and surname. FALSE*
- *If I don't put my name and surname on a forum, nobody will be able to identify me. FALSE*

Lesson 4
–
Digital footprint

This lesson builds on the previous one on online privacy. The aims of this lesson are to understand what a digital footprint is and to make the learners aware that their data is currency on the modern internet and that they are not the only ones who can share data about themselves.

The term 'digital footprint' has several practical meanings. In theory, it covers everything that remains online after a user's actions. It has to be understood in two ways: it is both the data that we leave behind when we use the Internet and the data that is stored by companies, such as the customer order database or their website behaviour. The digital footprint is left more or less consciously.

Trainers must explain to the learner that various entities are interested in the data that users leave on the web. They seek to collect as much of it as possible and, to this end, track online activity. Various tools are used for this purpose.

Another thing to focus on is profiling. This is a mechanism that involves categorising people according to characteristics and behaviour. Profiling can be encountered in social networks, which record user activity and then present tailored advertising as well as in various book, music and shopping services. Their operation is based on the analysis of users' decisions and the adjustment of proposed content to them. It should be noted that such profiling is sometimes useful, but always limiting.

MODULE	Types and identification of threats in the Internet	LESSON UNIT	4	TOPIC	Digital footprint

LEARNING OUTCOMES:

- Learners will become familiar with and understand the concept of digital footprint
- Learners will understand that information may not be shared online by themselves alone
- Learners will understand who may collect the data and for what purpose
- Learners will know that information cannot be removed from the internet
- Learners will know the consequences of using an Internet search engine
- Learners will know who may be interested in their personal information and what kind of information may be desired

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY discussion (time: 20 min)	Familiarising learners with the aims of the lesson, discussion on the availability of information on the Internet.	1. The trainer greets the learners. 2. The trainer defines the lesson aims and presents them to the learners. After today's lesson you will: • know what a digital footprint is • understand what information is being shared on the internet and what it can be used for • know what entities and organisations may be interested in information about you 3. The trainer acquaints the learners with the lesson plan and its subsequent stages.	• Computer, projector, internet access • whiteboard

		4. The trainer asks the group the following questions: • What information is available on the web about you? S/he writes down the answers on the board. • What data about your computer goes to the network? S/he writes down the answers on the board. 5. The trainer draws learners' attention (especially if it does not appear in the responses) to data such as geolocation data, computer IP address, type of web browser, operating system, place of logging into the network, etc. The trainer may point out that the individual data being sent to the network may not be of great importance, but when combined, it may be a real mine of knowledge about users. If the data is not recorded on the board, the trainer adds it.	
Task **TRY TO NAME (time: 20 mins)**	Learners will know who may be interested in their personal information and what kind of information may be desired Becoming familiarised with the concept of 'digital footprint'	1. Learners divide the information on the board into three categories: • automatically posted (browser, IP, system) • posted semi-automatically (location, information in photos about the date and time of taking them, the camera model) • posted by users themselves (forum entries, comments, e-mails, blog entries, YouTube videos) 2. The trainer asks the learners to think about what organisations might be interested in the information on the web.	• Computer, projector, internet access • whiteboard • computers for learners • Interactive quiz on information in the internet

		3. Learners solve the quiz - Information in the internet 4. The trainer gives a presentation summarising the interactive quiz, and the learners reflect on the purpose of a potential use of the information. 5. Learners together with the trainer explain the meaning of the term 'digital footprint'.	
Task **ACT (time: 20 mins)**	- Learners will see what the consequences of sharing data can be and how to minimise them	1. The trainer divides the learners into groups and distributes worksheets to each of them (see the e-book). The trainer asks each group to reflect on the answers and list such behaviours that would limit the amount of information disclosed about themselves on the Web. 2. The trainer asks the groups to present solutions. 3. The trainer summarises the activity.	• Computer, projector, internet access • whiteboard • Worksheets available in the e-book
Task **ACT (time: 10 mins)**	Learners will know the consequences of using an Internet search engine	1. The trainer asks the learners to reflect upon what queries they have recently entered into the search engine and what information the search engine can collect about them. 2. The trainer points out that, based on the actions related to the search engine- creating queries and entering individual links, Google creates a profile of the person, on the basis of which it presents search results tailored to the user. Thus, it can perfectly adjust the advertisements shown to us.	• Computer, projector, internet access

GOOD PRACTICES **(time: 15 mins)**		1. The trainer informs the learners that they can use browser plug-ins to check which entities track our activity, but they were not websites that had previously been opened. 2. The trainer acquaints the learners with the steps thanks to which the information sent to the internet can be limited.	• Computer, projector, internet access
FEEDBACK/ REFLECTION TASK (time: 5 mins)		1. The trainer summarises the lesson. 2. The trainer addressed the learner's questions. 3. The trainer encourages learners to make use of the next module on cybersecurity.	• Computer, projector, internet access
Self-study quizzes **Extended learning** **Consolidation**		As part of exploring the topic, learners can watch Gary Kovacs' speech "Tracking the trackers" https://www.youtube.com/watch?v=f_f5wNw-2c0 or Luka Crouch'a "How online trackers track you and what you can do about it" https://www.youtube.com/watch?v=jVeqAemtC6w	

There are two quizzes and a worksheet for this lesson:

Quiz 1

'Information on the web'. Interactive quiz needed for the second stage of the class. Solving the quiz is the basis for discussion with the learners and for joint definition of the term 'digital footprint'. The quiz involves matching the entity with data in which they may be interested. Below is the content of the quiz with sample answers. This is not the only correct solution. When discussing the activity, doubts may arise about the placement of data under the answers. The trainer should treat this as a starting point for discussion. Then students should focus on the ability to justify why an entity might be interested in collecting data. The trainer can ask the learners about the potential reasons certain entities collect data.

Question 1

Internet provider	**marketing company placing advertisements**
data transfer	search history websites visited

Question 2

server administrator	**marketing company placing ads**
data transfer IP address	YouTube videos viewed

Question 3

Blog owner	**mobile network service provider**
i number of visits to the website age of visitors	information about text messages sent hours of phone calls

Question 4

website with video content	internet provider
history of google searches history of videos viewed	IP address

Question 5

server administrator	website with music content
data transfer	searches for music bands watched video clips on video sharing portal

Question 6

marketing company doing market research	internet provider
items viewed in online auctions gender	amount of data downloaded

Worksheet to be printed or displayed on the board.

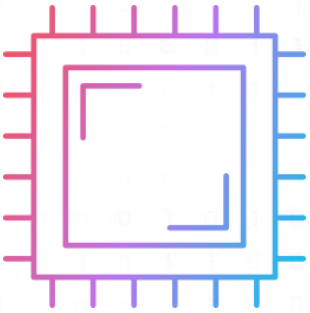
When working with it, different answers may also come up. The trainer should allow the learners to argue and explain their answers.

WORKSHEET for the lesson 'Digital footprint'
Instruction: Read the stories below and consider the answers to the questions Why does the behaviour described in the text not guarantee anonymity? What might be the consequences of such behaviour for privacy? In the situation described, how can one behave in order not to reveal so much information about oneself to others?
Situation 1 You would like to share photos of your birthday party with others. You post the photos on a social networking site. You and your friends are featured in the photos. You tag your friends. Your profile is public.
Situation 2 At work, you disagree with your manager's actions. In your opinion, your manager organises the work of your department poorly. You make an unflattering post on a social networking site about your manager and work at that company.
Situation 3 You are having a worse time in your life: a sad and difficult event has taken place for you. You decide to look for help on the Internet. You create an account on a portal offering psychological help by giving your name and describing the situation in detail.

Quiz 2

A quiz already known from previous lessons, in the form of ten questions to which learners answer TRUE or FALSE by ticking the appropriate boxes on the screen. The quiz with the correct answers is shown below. It can be used at the end of the lesson as a summary of what the learners should know after the lesson and can be done together, e.g. on an interactive whiteboard, or by each learner individually on their computers/tablets. Alternatively, learners can be asked to take the quiz themselves at home as a self-evaluation.

- *On the Internet you are completely anonymous. FALSE*
- *No one is interested in what I browse on the Internet. FALSE*
- *It is hard to predict the future consequences of posting different information about yourself online. TRUE*
- *The Internet provider does not collect any information about web users. FALSE*
- *The IP number is information that is automatically posted on the network. TRUE*
- *I have a say in shaping my digital footprint. TRUE*
- *All information can be effectively removed from the network. FALSE*
- *The type of an operating system is information that is posted automatically. TRUE*
- *The search engine does not remember the history of queries. FALSE*
- *It is not possible to locate the place where I use the computer. FALSE*



MODULE 2
–
COUNTERACTING AND MINIMISING RISKS AND ENSURING NETWORK SECURITY

Very time users connect to the internet through different types of devices, they are exposed to danger, which is why it is essential to ensure that they know how to navigate safely online.

In the first module, online risks were presented and identified. The learners are already aware of the different risks and can identify them. This module is intended to equip learners with knowledge and skills on how to counteract these threats. It is an extension of the lessons from module 1.

Module 2 includes 4 lessons on:

1. *how to effectively protect yourself from spam and scam messages and fake websites*
2. *how to recognise phishing messages effectively? How to protect yourself from phishing*
3. *how to take effective care of your privacy and data when using the internet*
4. *how to effectively protect yourself when using the internet*

Lesson 1

–

How to effectively protect yourself from spam and scam messages and fake websites

Spam and scam are common online threats. The lesson from module one showed how to identify these threats. The aim of this lesson is to make the learners aware of the essential risks present on the Internet and to develop skills to recognise and defend against scam and spam messages.

Before the lesson, trainers should prepare examples of scam messages that are popular in the countries concerned. These could be e-mail, SMS or instant messaging messages.

MODULE	Counteracting and minimising threats and ensuring network safety	LESSON UNIT	1	TOPIC	How to effectively protect oneself against spam and scam messages as well as fraudulent websites?

LEARNING OUTCOMES:

- Learners will understand the importance of awareness of the risks that are present in the Internet.
- Learners will know how to recognise spam and scam messages and identify fake websites.
- Learners will know what tools to use to protect themselves from spam and scam messages and fraudulent websites.
- Learners will know examples of good practices to protect against spam, scam and fraudulent websites.

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY (time: 20 mins)	Presentation of examples of spam and scam messages and fraudulent websites.	1. The trainer presents the lesson objectives and the plan as well as explains to the learners that during this lesson they will: • understand how important it is to be aware of the risks when using the Internet, • learn how to recognise spam and scam messages and identify fraudulent websites, • learn the methods and tools that should be used to protect themselves against spam and scam messages and fraudulent websites, • learn about examples of good practices of protection against spam and scam phenomena as well as fraudulent websites.	• the presentation • projector and computer with Internet access for the trainer • prepared sets of spam, scam and phishing emails • prepared sets of exemplary fraudulent websites and links

		2. The trainer reminds the basic concepts of spam, scam and fraudulent websites. 3. The trainer presents sets of spam and scam emails and examples of fraudulent websites. 4. In pairs, learners classify sets of e-mail messages as: regular e-mail, spam or scam. They also analyse the examples given and the links to websites that may be classified as fraudulent websites. 5. The learners explain what made a given email message or website eligible for a given category.	
Task **TRY TO NAME (time: 25 mins)**	Learners indicate the characteristics of spam and scam emails and suspicious features that can be found on fraudulent websites.	1. The trainer discusses with the learners how criminals can use our own inappropriate behaviour when using e-mail and browsing the Internet. The trainer asks whether the learners themselves receive such messages. 2. The trainer asks the learners to log into their personal e-mail accounts and check if there are also spam or scam emails among the messages. 3. The trainer summons up practical examples of cyber-attacks based on spam and scam emails and examples of using fraudulent websites. The trainer provides links to information about the attacks in question. 4. The trainer asks for the characteristics of spam and scam emails and how fraudulent websites are used. 5. The trainer provides statistics and data on spam in recent years and points to the use of spam and scam messages as	• the presentation • work with computers-learners have access to computers with the Internet access • practical examples of cyber-attacks based on spam and scam emails and examples of fraudulent websites • statistics and data on spam in recent years

		a means to steal data of users of websites and internet portals and to access electronic banking.	
Task **ACT** **(time: 25 mins)**	Learners will become familiar with methods and tools to protect against spam and scam emails and fraudulent websites. Learners will learn to use the tools presented in the class.	1. The trainer presents an activity demonstrating the application of methods and tools to protect against spam and scam emails and fraudulent websites. 2. The trainer presents the method of protection, including e-mail account, e-mail software, browser, use of temporary addresses as well as additions and filters. The trainer introduces and shows how to use the recommended software and settings. 3. The learners evaluate the solutions used in the activity. Discussion. 4. The trainer discusses the individual elements of the activity with the learners, explaining why a given action is important from the point of view of protection against spam and scam emails and fraudulent websites. 5. In pairs learners choose the software and methods that should be used in their case from the presented catalogue.	• the presentation • work with computers-learners have access to computers with the Internet access • a prepared activity demonstrating the use of methods and tools to protect against spam and scam emails and fraudulent websites. • a prepared printout of the catalogue including recommended methods, procedures and software to protect against spam and scam messages and fraudulent websites

GOOD PRACTICES (time: 15 mins)	Learners will become acquainted with a list of best practices that support protection against spam and scam messages and fraudulent websites.	The trainer gives an example of good practices protecting against spam and scam messages as well as fraudulent websites. S/he distributes a list of good practices to learners and discusses the more important tools and methods for countering threats and cyber-attacks on the Internet.	• the presentation • a printout of the catalogue including recommended methods, procedures and software to protect against spam and scam messages and fraudulent websites
FEEDBACK/ REFLECTION TASK (time: 5 mins)	Learners' enquiries on the issues discussed. Summary of the lesson.	The trainer emphasises the ability to recognise spam and scam messages as well as fraudulent websites in the context of ensuring a higher level of cybersecurity. The trainer addresses any questions from learners and summarises the lesson.	• the presentation

The trainer should provide the learners with a list of good practices to help them protect themselves from scam and spam messages.

1. *Do not naively believe that everything you see on the internet is true. Remain vigilant and use common sense.*
2. *Install tools to strengthen your online security. Anti-virus software is a must, but consider additional security features as well.*
3. *Update the software installed on the devices you use to access the Internet on a regular basis.*
4. *Check your spam filters. These are created and configured by the administrators of the servers where email accounts are set up. Before deciding on a particular platform, check what anti-spam protections are in place on that platform.*
5. *Avoid registering with untrusted services, providing your email address when registering with some services may lead to your email address being spread and receiving email spam.*
6. *Do not reply to suspicious e-mails. Do not trust phone calls or messages encouraging you to invest, especially if you do not know the caller or sender of the message. Be suspicious when someone offers you a guarantee of large profits.*
7. *Use different email addresses. You may use temporary email addresses to register an account on some sites.*
8. *Never share your personal information.*
9. *If you have any doubts, contact the relevant services.*

Two interactive quizzes have been prepared for the lesson.

Quiz 1

The quiz presents the most common online scams. Learners can familiarise themselves with scams they may encounter online. The quiz is for use as a presentation during the second stage of the lesson, in which the trainer brings up practical examples of cyber attacks. This is also a good time to discuss with learners about their experiences with scam attacks. It may be that they have already had contact with this form of scam or have heard about it among their family or friends. It should also be pointed out to the students that the victims of attacks are most often ordinary people. Below the content of the online exercise is given:

The most popular online scams:

1. *Promise of quick money and bargain shopping*

This type of scam often begins with a phone call, message on social networking sites, instant messaging or email advertising a job that requires no special training or qualifications, but offers high profits in a short period of time. In bargain shopping, criminals often use the bargain low price of a product or service offered for purchase online as a lure.

2. *Online grooming*

Cybercriminals use acquired online dating acquaintances to gain the victim's trust and thus cheat them out of money or personal information. The scammer often strikes up a conversation and then starts an online relationship with the victim. The scammer invents reasons to ask the victim to hand over money (e.g. for medical expenses).

3. *Forcing ransom and threats*

Ransom extortion is a way for the scammer to withhold allegedly embarrassing information about the victim's life or the victim's family member. Often, the fraudster actually gains access to information, photos or videos posted on social media, so that the ransom demand and threats sent become real

4. *Taking over identities on social networks*

In addition to the classic takeover of a social networking account, social profile cloning (i.e. using the name, photos and information from a real account to create a second almost identical profile for use in planned scams) is also encountered. Frequently, the scammer sends invitations to friends from the list of the original account in an attempt to gain access to the data of further potential victims. The scammer exploits the trust of the victim's friends, e.g. by sending them messages with fake links.

5. *Fake online shops*

Fraudsters create fake online shops that either look authentic or are perfect copies of real sites. Attractive low prices of the goods offered by the scammer are often a lure. This allows them to gain a large number of customers before their scam is detected

6. *Phishing scams*

A scammer sends you a message that appears to come from a legitimate source, such as a bank, courier company, social network or online shop. In the message, you receive info that requires you to log into your account or provide financial details. The pretext may be that the terms and conditions have changed or that you need to pay a small amount extra for your order. The whole phishing message is made to look urgent and at the same time easy for the victim to follow the scammer's instructions without thinking.

7. *Lotteries and attractive prizes*

You receive a message from the scammer via email or social media with information about an attractive material prize, the possibility of winning a large amount of cash, a free trip or a reward for completing an inoculation. The scam is set up in such a way that claiming the promised prize or taking part in the competition or lottery only requires the victim to register and provide their details or pay a small amount for processing fees etc.

8. *Distribution of malicious software*

Malware is often designed to scan a phone or computer for personal and banking information, log keystrokes, block access to a device, access a camera or encrypt all the victim's data. More often than not, malware distribution starts with the victim's inattention and clicking on a fake link in an email, opening an attachment with a hidden virus or installing a programme from an untrusted source.

9. *Fake IT support services*

This type of scam usually begins with advertisements of false offers of services related to all kinds of computer, smartphone and software support. Virtually every form of this scam requires the victim to install remote access software, allowing the perpetrator virtually unlimited access to the victim's computer

10. *Fake financial services*

Fake financial services include both fake login pages for banking services (involving attempts to access the victim's bank account) and fake payment intermediary pages (e.g. Paypal, Multibanco, PayU, Nexi). The attack is usually carried out via a link (sent e.g. in an email or instant messenger) leading to a fake site that aims to take over the victim's login and password.

Quiz 2

This quiz introduces different types of Nigerian scams. Learners can display this quiz as a summary of the lesson at the end of class or at home as a trivia activity.

The most common types of Nigerian scams involve:

1. *Receiving a large inheritance*

In this scheme, the potential victim is told that he or she is the heir of a very rich distant relative who has recently died. In order to receive a large sum of inheritance money, only small administrative and court costs need to be paid. The scammers describe the alleged problems and encourage the victim to make payments to speed up the inheritance procedure.

2. *Participating in an auction of valuable items*

The offer made by the fraudsters contains information about a unique opportunity for the victim to earn a lot of money. This opportunity is supposed to be an auction of, e.g., precious stones or antiques at a very attractive price. The bidding, where the victim supposedly wins the auction, takes place on a fake website. Time is of the essence and the scammers encourage the victim to make a payment as soon as possible.

3. *An ownerless bank account*

In this case of fraud, we usually receive a message from an employee of the bank where there is an account with a large sum of money to be transferred to the addressee of the message. The fraudster assures us that the money already belongs to us, but that the transfer will be ordered to the victim's account after a small payment has been made for tax or bank charges.

4. *Winning a lottery or payment of compensation*

The victim receives a notification of a lottery win or information about a pending compensation payment. The scammer encourages the victim to claim the

prize (e.g. a large sum of money or jewellery) if he or she covers the prize tax or shipping charges.

5. *Participation in an investment*

The incredible opportunity to earn very large amounts of money by contributing to a special investment fund is presented in the message. The victim is promised high returns and a guarantee of the safety of the invested money. Often the incentive to invest is to be found in the stories of other people who have multiplied their wealth in this way.

6. *Assistance to a political refugee*

A political refugee persecuted by the regime and in need of help writes to the victim of the scam. Often at first the criminals ask for small deposits of money, but over time their demands increase. In emotional messages, they write about the political struggle and the threat to the health and lives of the regime's opponents in order to evoke pity and encourage the victim to make further payments of money.

Lesson 2

-

How to recognise phishing messages effectively? How to protect yourself from phishing

Phishing is a method of fraud that involves impersonating a credible source, such as a bank, in order to extract important information such as credit card details, personal data or security passwords, and the attack is usually carried out by sending out fake emails.

The students learned what phishing is and how it works in the first module. Now they will learn how to recognise phishing messages and how to effectively protect themselves from attacks.

The most common phishing scams vary from country to country, therefore the trainer should do some research on phishing in their country before the lesson. Fraudsters often impersonate trusted public institutions. In order to obtain data, they rely on the weakest link of protection, the human being, and invoke the power of habit.

MODULE	Counteracting and minimising threats and ensuring network safety	LESSON UNIT	2	TOPIC	How to effectively recognise phishing emails? How to protect oneself from phishing?

LEARNING OUTCOMES:

- Learners will know how to recognise a phishing email
- Learners will know how to respond to suspicious phishing emails
- Learners will know how to recognise a phishing message sent to a messenger or via SMS / MMS
- Learners will understand the importance of verifying the sender and content of suspicious messages
- Learners will know where to look for tools and information to verify the sender and content of suspicious messages

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY (time: 15 mins)	To present sample e-mails and messages from instant messaging and texts / mms with phishing content	1. The trainer presents the lesson objectives and plan as well as explains to the learners that during this lesson they will: • learn how to recognise phishing messages sent by e-mail, instant messaging or via text messages or mms, • understand how to react to suspicious phishing emails • understand the importance of verifying the sender and the content of suspicious messages	•the presentation •a set of printed suspicious messages •a set of suspicious messages in an electronic version •a projector and a computer with internet access for the trainer

		• learn where to look for tools and information to verify the sender and content of suspicious messages. 2. A reminder of the definition of phishing and its types, discussed in the previous module. 3. The trainer asks learners to read the provided sample of phishing messages and regular messages, e.g. advertising messages. They analyse the messages on their own for about 5-10 minutes. Suspicious messages also include "regular" non-threatening messages that learners should recognise.	
Task **TRY TO NAME (time: 15 mins)**	Based on their knowledge, learners are to classify the messages as those of a phishing nature	1. The trainer asks for the first observations as to the content and form of the message. Learners' comments. 2. The trainer asks them to qualify the messages because of suspected phishing and its types (phishing, spear phishing, clone phishing, whaling, pharming, text message / mms phishing, voice phishing). 3. Moderated initial message analysis by learners 4. The trainer asks the learners whether they, their friends or family have received similar phishing messages. 5. The trainer provides examples of phishing activities and their reliance on social engineering.	•work with computers •learners have access to a computer with the Internet •a set of printed suspicious messages •a set of suspicious messages in an electronic version •the presentation

Task **ACT (time: 45 mins)**	To make learners familiar with ways how to verify suspicious phishing emails based on a checklist. To make learners independently evaluate and verify phishing emails.	1. The trainer presents a checklist of questions that will be the basis for the analysis of individual messages in terms of phishing. The questions in the event of suspected phishing messages are the basis for the statements of individual learners who evaluate a specific suspicious message. 2. The trainer discusses the subsequent questions and provides examples illustrating the issues of a given question, e.g. suspicious phrases or link redirection. Then the learners check whether the messages provided to them at the beginning of the class have a phishing nature based on the questions from the checklist, and make an assessment and verification. 3. The trainer points out to the learners that among the control questions there are issues related to the uncertainty as to the identity of the message sender. The trainer acquaints the learners with the information concerning the data contained in the message header and the rules which enable the analysis of the email message header. 4. The trainer shows how to check the message header with the use of verification tools, and then discusses the obtained results. 5. Learners in pairs check the headers of ordinary messages. The trainer supervises the activity and provides support.	•the presentation •work with computers •learners have access to a computer with the Internet •a checklist of questions to verify if we are dealing with phishing •a list of links to tools that verify email headers •regular email headers for learners to analyse •suspicious email headers for learners to analyse

		6. Learners in pairs check the prepared headers of phishing emails. Pairs present and discuss the obtained results.	
GOOD PRACTICES (time: 7 mins)	To make learners acquainted with a list of good practices against phishing.	The trainer provides an example of good practices on how to protect oneself from phishing. S/he hands out a list of good practices to learners and discusses the individual points.	•the presentation •the printed list of good practices against phishing.
FEEDBACK/ REFLECTION TASK (time: 8 mins)	To revise and verify the acquired knowledge.	Learners check the acquired knowledge and skills by taking a quiz.	•the presentation •work with computers •participants have access to a computer with the Internet •link to the quiz "Do you recognise phishing?"
Self-study quizzes **Extended learning** **Consolidation**	To summarise	The trainer summarizes the lesson.	

In the third stage of the lesson, the trainer presents a list of screening questions that will form the basis for analysing individual messages for the existence of phishing. The list of questions is shown below. Nevertheless, if the trainer has some free time in the lesson, they can encourage the learners to try to create such a list. Learners have seen examples of fake emails and websites before and, based on their experience, can determine what questions they would ask themselves if they wanted to verify whether a message is fake. The trainer can then supplement such a list.

List of questions to verify if we are dealing with a case of phishing:

1. *Do I recognise the sender of the email?*
2. *Does the sender's email address come from a suspicious domain?*
3. *Is it an unexpected message containing links or attachments?*
4. *Does the email have a subject line that is irrelevant or inconsistent with the content of the email?*
5. *Is the email in response to something I never sent?*
6. *Has the sender included an attachment with a potentially dangerous file type?*
7. *Is the email unusual, containing grammatical or spelling errors?*
8. *Is the sender asking me to click a link or open an attachment that seems strange or illogical?*
9. *Does the message ask me to enter my details, log in to my bank account or another service?*
10. *Is there pressure in the message to transfer money or pay some fee as soon as possible?*

The same applies to the 'good practices' part of the activities. Trainer could try to make such a list with the learners, so that the ideas for good habits come from the learners themselves. The trainer can use the brainstorming method here and write down the ideas that come up in the group. At the end, the lesson should simply be summarised and the group work completed, if necessary. Alternatively, Trainer may give the learners a ready-made document and just discuss it with them.

Good online habits:

1. *Never open messages that seem suspicious to you. Always pay attention to the sender of the message and the headline.*

2. *Be vigilant if you spot spelling mistakes and typos in an official message.*

3. *Never reply to an e-mail that appears suspicious to you. Ignore requests for your login and password, your personal details or a scan of your ID.*

4. *Do not trust messages asking for money - even from close friends or colleagues. Remember that their account may have been hacked and used against their intentions.*

5. *Refrain from downloading or opening suspicious attachments. Downloading files from unknown sources is extremely risky.*

6. *Never click on suspicious links. Hover over the link with your mouse and see where it leads. Check the web address carefully and make sure it is secure.*

7. *Do not email confidential data or information about your bank account or passwords.*

8. *If you are in any doubt as to whether a message is actually from a particular company or institution, contact a representative of that company or institution via another communication channel or seek confirmation of the information from other sources.*

9. *Report any website, e-mail or SMS messages that may be fraudulent to the relevant institution.*

There are two interactive exercises for this lesson plan too.

Quiz 1

This quiz will be a great activity to wrap up the lesson. It provides links to resources where learners can test their own knowledge and skills about phishing. Using the links provided in the exercise, they may verify whether they can recognise a phishing scam attempt or not.

Test your ability to recognise phishing.

1. *All phishing attacks are very similar to each other. They have one thing in common: the use of the human factor and social engineering to trick unsuspecting victims. See if you can recognise suspicious messages:*

   Link to resource: https://phishingquiz.withgoogle.com/

2. *Attackers know exactly how to write a message in order to arouse emotions in the victim that lead them to act quickly and recklessly. Scammers are getting more and more creative, so we can expect an attack at almost every turn. See if you can spot the threat:*

   Link to resource: https://www.phishingbox.com/phishing-iq-test

3. *Criminals using phishing attacks like to impersonate well-known companies, financial institutions and authorities. Can you tell the difference between a real message and a phishing message?*

   Link to resource: https://www.sonicwall.com/phishing-iq-test-landing/

Quiz 2

This quiz can be used at the end of the lesson. It contains the names of different types of phishing. The task is to match the name with a description of the attack. The content of the exercise is shown below:

- *Phishing attacks are very similar to one another, but they have one thing in common: the use of social engineering that facilitates the phishing of data from unsuspecting victims.*
- *Personalised attacks targeting specific web users are particularly unpleasant. Such activities known as SPEAR-PHISHING are harder to detect and much more effective because fraudsters collect data on potential victims and carefully select the target of the attack.*
- *A common form of attack is for the attacker to copy a real email very precisely in order to lull the victim's alertness and encourage them to click on false links leading to a malicious site. This form is called CLONE-PHISHING.*
- *The type of personalised attack that seeks to capture data from the most senior people in a company is called WHALING.*
- *A type of phishing that involves spoofing a domain or phone number. A cybercriminal using SPOOFING impersonates an existing domain or a phone number in order to make their email or phone call look real.*
- *An attack using a text or MMS messages containing a malicious link is classified as SMISHING.*

Lesson 3

–

How to take effective care of your privacy and data when using the internet

Online security and privacy are two priority elements that are mostly overlooked or neglected by users. The benefits of using the web can overshadow security and privacy issues. Using the internet and enjoying its many facilities can be safe, but it is essential to remember a number of important elements. A key objective of this lesson is to acquire the ability to recognise privacy and data risks and to learn how to protect one' s privacy online.

Trainer can use quiz 1 from the third lesson of the first module to remind students of the concepts of privacy, personal and sensitive data that were discussed in the previous module. In order to conduct the lesson effectively, to illustrate all aspects of the lesson to the learners, the trainer should prepare in advance an email account and a social media account with the data of a sample user.

MODULE	Counteracting and minimising threats and ensuring network safety	LESSON UNIT	3	TOPIC	How to effectively take care of one's privacy and data while using the Internet?

LEARNING OUTCOMES:

- Learners will know what data is collected when we use the internet.
- Learners will understand how important it is to be aware of the risks to privacy and data that we leave online.
- Learners will know how to recognise threats to their privacy and data.
- Learners will know how to protect their privacy online.

ETAPY	CELE	PROCEDURA	ZASOBY
CASE STUDY (time: 25 mins)	To present an exemplary set of information collected about a specific Internet user	1. The trainer presents the objectives of the lesson and the lesson plan and explains to the learners that during this lesson they will: • learn what data is collected when we use the Internet, • understand how important it is to be aware of the risks to privacy and data that we leave online, • learn to recognize threats to their privacy and data, • learn the methods of protecting their privacy and data on the Internet.	• the presentation • a prepared Google account with the data of an exemplary user • a prepared Facebook account with data of an exemplary user • a list of 98 pieces of information that Facebook makes available to advertisers • a projector and a computer with internet access for the trainer

		2. Reminding the scope of the concept of privacy, personal data, and sensitive data discussed in the previous module. 3. The trainer presents what data is collected by selected service providers (Google and Facebook), including: location data, activity in the web and applications, search and purchase history. 4. The trainer presents a list of data collected by Facebook and made available to advertisers. The categories of data and the sources of their acquisition are discussed.	
Task **TRY TO NAME (time: 25 mins)**	Learners are to enumerate what threats may appear to the privacy and data that we disclose on the Internet.	1. The trainer asks about the risks associated with so much data that we leave on the web. Discussion. 2. The trainer discusses with the learners how criminals can use the data, both those that we leave unprotected in the network, and data stolen by, for example, a phishing attack. The trainer provides specific examples of the use of data by criminals. 3. The trainer asks learners to indicate what data we most often provide during registration. Moderated discussion based on examples provided by learners and their experiences during registration, setting up accounts on websites.	• work with computers • learners have access to a computer with the Internet learners find on the Internet documentation on the privacy policy of selected websites and suppliers (e.g. Google, Microsoft, Apple, Twitter, Yahoo, Vimeo, Netflix) • the presentation

		4. The trainer introduces the concepts of the privacy policy. Together with the learners, they analyse the information they find.	
Task **ACT (time: 30 mins)**	Learners are to know the profiling phenomenon and what to do in the event of a data leak.	1. The trainer presents the concept and procedure of the so-called "Right to be forgotten" and resembles the GDPR regulations. 2. The problem of profiling network activity is discussed. 3. The trainer asks learners whether they themselves (or their friends) have been victims of personal data leakage and breach of privacy on the Internet. 4. The trainer provides examples of data leaks and privacy breaches and presents the scale of cyber-attacks, often aimed at stealing data of website and portal users. 5. The trainer presents an exemplary catalogue of actions that should be taken by the user in a data leakage situation.	• presentation of a pattern of activities under the "right to be forgotten" • sharing links regarding user data leaks • presenting a catalogue of actions to be taken by the user in the event of a data leak • work with computers • participants have access to a computer with the Internet • the presentation
GOOD PRACTICES **(time: 8 mins)**	To make learners acquainted with a list of good practices in the field of privacy and data protection on the Internet.	The trainer provides an example of good practices in the field of privacy and data protection on the Internet as well as distributes a list of good practices among learners and discusses the main points.	• presentation • a printed list of good practices in the field of privacy and data protection on the Internet

FEEDBACK/ REFLECTION TASK (time: 2 mins)	To address learners' questions on the issues discussed. To summarise the lesson.	The trainer emphasises the special nature of privacy and data in the digital world and answers any questions from the learners. At the end, the trainer summarises the lesson.	• presentation

In order to conduct the lesson, the trainer will need a number of more things, one of them being a list of 98 pieces of information that Facebook provides to its advertisers about its users. The list is very easy to find online and can be found in English at the following link, among others:

https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/.

In addition to this, the lesson refers to a sample catalogue of actions that a user should take in a data leakage situation. We will define a data leak as an incident that results in the unintentional or intentional disclosure of data. Depending on the group the trainer is working with, the learners themselves can propose actions that should be taken after a data breach. It is possible to distinguish the three most important steps to be taken after being informed of an incident. If the leak involved login credentials, the first step is to log out and change the access password, using two-step authentication if possible. The second step should be to block the documents at the bank and the third step should be to report the incident to the relevant services.

Good online privacy and data protection practices:

1. *Use different, complex passwords. Do not use one password for several accounts.*
2. *Fill in web forms carefully and never give out data that is not required.*
3. *Block apps on your phone from tracking your location.*
4. *Never upload compromising or intimate photos on social media. Most things stay on the internet forever.*
5. *Never leave your data on websites that have no encrypted connection*
6. *Regularly clear your browsing history and delete cookies.*
7. *Limit your use of Wi-Fi in public places. Never log into your email or bank account from someone else's computer.*
8. *Never store valuable, sensitive data in the cloud.*
9. *Install anti-virus and pop-up ad blocker software on your computer.*

Two quizzes are provided for the lesson.

Quiz 1

Collects links to web resources where learners can check if their email address has been involved in any data leaks. The quiz can be presented in class or learners can be asked to check these sites at home and possibly share the results. The content of the quiz and the resources in it are presented below.

1. *Data leakage is a serious threat to our privacy in the Internet space. It can occur as a result of an attack by hackers who break security and access a company or institution's database. Unfortunately, it also happens that data leakage occurs as a result of human error when the person responsible for security fails to fulfil their duties. There are reports in the media about further leaks from websites or institutions. The scale of the risks associated with data leakage can most easily be seen by obtaining information about the largest such incidents.*

   Link to resource:

   https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

2. *Have I Been Pwned? is a website that allows users to check if their data has been compromised in a data leak. The website collects and analyses data that has been accessed as a result of a data leak and allows the user to search for information about the leak of their own data after the user enters an email address or phone number. The user may also be notified if their email address appears in future leaks.*

   Link to resource:

   https://haveibeenpwned.com/

3. *Firefox Monitor is a website that is a valuable resource for anyone wishing to protect their security and privacy. Firefox Monitor alerts you if your web service accounts have been exposed to a data leak. Find out if your information has been exposed in a data breach, learn what steps to take to better protect your online accounts and how to set up an alert if your email address appears in a new leak.*

   Link to resource:

   https://monitor.firefox.com/

Quiz 2

The information in this quiz shows students what privacy risks smart home products can pose. In many homes there are electronic devices that everyone uses but fails to think about the safety of their use. The quiz aims to make the learners aware that also the unskilful use of home electronic devices can endanger their privacy. The quiz can be used in class and displayed on an interactive whiteboard, for example. Alternatively, you can ask learners to think about the dangers of a particular device on their own and then check their answer against the explanation in the quiz. Quiz content:

1. ***Smart vacuum cleaner***

Explanation:

With the help of sensors, it reproduces the floor plan of the home, its surface area and the distances between furniture and appliances. The device records user activity in the home. The vacuum cleaner manufacturers have announced that they are considering making flat floor plans available to other players in the smart home industry. With this data, companies could recommend their products to users, e.g. furniture, cleaning products, etc.

2. ***Children's room camera***

Explanation:

It has the function of transmitting video and sound from the room where the child is staying. It can also transmit the signal in the opposite direction. With this type of device, there have been many cases of data leaks and hacking attacks due to poor security and lack of data encryption and software updates.

3. ***A voice-controlled smart speaker through which a voice assistant communicates.***

Explanation:

The manufacturers ensure that the speaker only starts listening when the user utters a key word. However, already in 2018, one device recorded a private conversation of its user without their consent, and the recording was then

automatically sent to a random person in the contact list. Some manufacturers offer a wider range of services offered by the device (e.g. heating control), but in return expect the participant to agree to continuously monitor the user's conversations to pick up product feedback and then better personalise advertising content.

4. ***Smart TV set***

Explanation:

As a default, some manufacturers left settings that allowed the TV to collect data on everything the user watched. The data collected was sold to advertisers who, through the IP address, were able to integrate it with their information on the same individuals. There were also failures to update the TV's software, which resulted in exposure to hacking attacks and, e.g., taking control of the microphone and camera.

Lesson 4

–

How to effectively protect yourself when using the internet

In the last lesson of the second module, students will learn how to recognise cyber security threats, learn about methods and tools to increase the level of internet user's cyber security and learn about examples of good practices to increase cyber security when using the internet. The trainer can start the lesson by explaining the concept of cyber security and mention that cyber security works like traditional security, but its purpose is to keep users and their computer systems safe.

The first stage of the lesson refers to an online cyber security self-assessment test. Quiz 1 described in the lesson plan can be used as a test here.

MODULE	Counteracting and minimising threats and ensuring network safety	LESSON UNIT	4	TOPIC	How to effectively ensure your cybersecurity while using the Internet?

LEARNING OUTCOMES:

- Learners will know how to recognise threats to the Internet user
- Learners will understand the importance of being aware of the risks present on the Internet
- Learners will know what tools to use to increase their cybersecurity on the Internet
- Learners will know examples of good practices increasing cybersecurity while using the Internet

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY (time: 20 mins)	Presentation of the self-assessment test of an Internet user's cybersecurity.	1. The trainer presents the lesson objectives together with the lesson plan and explains to the learners that during this lesson they will: • understand how important it is to be aware of the risks while using the Internet, • learn to recognise cybersecurity threats, • learn about methods and tools to increase the level of the Internet user's cybersecurity and will be able to apply them, • learn about examples of good practices that increase cybersecurity when using the Internet. 2. Reminder of the basic concepts regarding Internet threats. 3. The trainer presents a self-assessment test of Internet cybersecurity that allows each learner to assess	• the presentation • whiteboard • a projector and a computer with internet access for the trainer • preparation of the self-assessment test of an Internet user's cybersecurity

		which of their current behaviours increase the risk when using the Internet. 4. Learners individually complete the self-assessment test of Internet cybersecurity. 6. The trainer and learners indicate what threats may be caused by inappropriate behaviour described in the self-assessment test. The trainer writes down the answers on the board in the following layout: inappropriate behaviour- threat to cybersecurity.	
Task **TRY TO NAME (time: 20 mins)**	Learners indicate what actions lead to a threat to security when using the Internet.	1. The trainer discusses with the learners how criminals can use our own inappropriate behaviour to launch cyber-attacks. 2. The trainer asks the learners to indicate what behaviours can protect the Internet user from the threats listed on the board. 3. The trainer cites practical examples of threats and cyber-attacks on internet users, and then asks the learners to indicate what security measures should be taken when using a computer, smartphone, web browser, e-mail, online shopping and payments, and online banking. 4. The trainer asks whether the learners themselves or their friends have been victims of cyber-attacks. 7. The trainer discusses the scale of cyber-attacks, often aimed at stealing user data from websites and portals as well as access to electronic banking.	• whiteboard • presentation • practical examples of threats and cyber-attacks on users using a computer, smartphone, web browser, e-mail, online shopping and payments, as well as online banking • statistics and types of cyber-attacks in recent years
Task	Learners will become familiar with methods and tools to increase	1. The trainer presents an activity on how to practically ensure one's cybersecurity and data while using the	• presentation

ACT (time: 30 mins)	security and protection against cyber-attacks. Learners will be taught to use the tools presented during the lesson.	Internet. The learners evaluate the solutions used in the activity. 2. The trainer discusses with the learners the particular elements of the activity, explaining why a given action is important from the point of view of cybersecurity and data protection. 3. The trainer introduces and demonstrates how to use the recommended software that protects us against cyber-attacks. 8. In pairs learners choose from the presented directory software and applications that should be installed on the computer or smartphone of each internet user who cares for their privacy and wants to be protected against cyber-attacks.	• work with computers- learners have access to a computer with the Internet connection • it is possible to use the learners' smartphones with Internet access via Wi-Fi • a prepared activity on how to practically ensure one's cybersecurity and data while using the Internet, including the use of methods, procedures and software • use of the directory from the repository https://prism-break.org/pl/all/
GOOD PRACTICES (time: 15 mins)	Learners will become acquainted with a list of good practices increasing the level of cybersecurity when using the Internet.	The trainer provides an example of good practices increasing the level of cybersecurity when using the Internet. S/he distributes a list of good practices to learners and discusses more important methods of counteracting threats and cyber-attacks on the Internet.	• presentation • a printed list of good practices increasing the level of cybersecurity when using the Internet
FEEDBACK/ REFLECTION TASK (time: 5 mins)	Learners' questions on the issues discussed. Summary of the lesson.	The trainer emphasises the importance of the ability to recognise and counteract threats using the known cyber security tools. The trainer answers any questions from learners and subsequently summarises the lesson.	• presentation

There are two quizzes for this lesson:

Quiz 1

This is a short test on online safety. The learner's task is to answer the quiz questions according to how they behave online. The quiz will add up the points in all the answers and the learner will be able to see to what extent they take care of their digital security. The quiz should be taken individually by each learner on their computer or tablet. It is designed to be displayed and taken in the first stage of the lesson, while introducing cyber security issues. Questions included in the quiz are as follows:

1. *Passwords for my accounts (e.g. computer, email account, social networking site, auction site) are usually:*

    a) short and simple (e.g. same as login, date of birth, pet name, single word)

    b) the same password as for other services with a different number at the end, because I use the same password for many accounts

    c) long, consisting of upper- and lower-case letters, as well as numbers and non-alphanumeric characters or a long phrase, I use a different password for each account

2. *Do I log on to any of my accounts in a public place using a public Wi-Fi access point?*

    a) very often

    b) sometimes

    c) never

3. *Do I enter my real data when using Internet resources?*

    a) always when the site asks for it (e.g. taking part in competitions)

    b) sometimes

    c) only when it is necessary and essential (e.g. shopping)

4. Do I use an anti-virus programme on my computer with an up-to-date database as well as the recommended security-sensitive browser extensions?

a) I do not use any of the above

b) I use some of them, but I don't always remember to update them

c) I use all of them

5. When someone sends me an e-mail, link or an attachment I open it:

a) always and from anyone

b) sometimes, but the e-mail must be addressed to me directly

c) only if it is sent by a friend and looks plausible – if in doubt I check the link

6. I have an antivirus program installed on my smartphone:

a) no

b) I don't know

c) yes

7. When shopping online:

a) I don’t think about security because I care about time

b) I always look for the cheapest offer

c) I try to check the shop’s terms and conditions and customer reviews and I pay attention to which site my payment is made on

In the test, by default, answer C is correct - it describes the optimal action in terms of security.

Feedbacks:

21-19 - You are a conscious user, you take care of your safety on the Internet. You can take care of your data and privacy online, you avoid unnecessary risk in public Wi-Fi access points and you properly secure your computer and smartphone. You can avoid threats when using Internet resources but be careful: you have to be cautious because new cyber-threats appear every day!

18-16 - You need to pay more attention to your cybersecurity when using the Internet. Although you have good habits when using Internet resources, there are situations when you clink an unknown link without thinking or you forget to update your software. You know a lot about cyber-threats but you can always raise your knowledge to a higher level.

<15 - Your data isn't safe on the Internet. You have to pay more attention to what you click on and which data you share. You need to work on your safety on the Internet. You are often exposed to cyber-threats due to your actions. Start using good practice for cyber-threats, for example when using public Wi-Fi access points or opening attachments in emails.

Quiz 2

This is an educational support material that the trainer can use in class or as a resource for the learner to do individually at home. The quiz collects various tools that can help the web user take care of their own safety. Thanks to the quiz, learners will have easy access to online tools to increase their cyber security. A list of resources presented in the quiz is presented below:

1. VirusTotal is a helpful tool for assessing threats in the form of suspicious attachments or links arriving in email inboxes from the Internet. It is used by both individuals and professionals fighting malware. The idea behind it is very simple – you point to a suspicious file or paste a link to a page and receive feedback on it from approximately 70 different antivirus engines.

   Link to resource: https://www.virustotal.com/

2. Find out how you can change the settings of your online services to take control of your data and increase security.

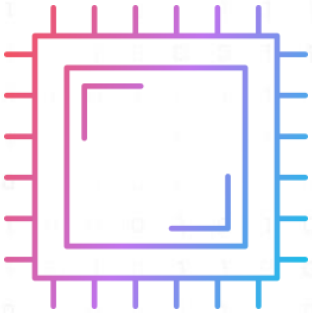
   Link to resource: https://privacy.kaspersky.com/

3. Check your password for security and the possibility of cracking it with a brute force attack. In addition, the service allows you to check whether the password you are using can be found in a database of published passwords.

   Link to resource: https://password.kaspersky.com/pl/

4. See a comprehensive guide to increasing your online security and privacy. The catalogue also includes suggested software.

   Link to resource: https://prism-break.org/en/



MODULE 3
–
ACTIVE PARTICIPATION IN THE INFORMATION SOCIETY

Information technology offers increasingly improved and sophisticated social communication tools. We use social networking sites, various instant messaging services and e-mail on a daily basis. Young people are more likely to use the resources of the Internet than traditional information media such as television, radio or books.

An information society is a society benefiting from technologically advanced means of collecting, searching for and processing information and communication. The term itself can be treated as a kind of mental shortcut, being only one of the attempts to define the most important features, mechanisms of functioning and effects of contemporary phenomena related to the development of information technologies. There is no doubt that there is the development of the Internet behind the emergence and development of the information society. In the information society, information technology is used in almost every area of social or personal life, and the standard of living is determined by access to information resources.

The following lessons are included in Module 3 "Active participation in the information society":

1. *Digital identity and mobile media*
2. *Remix – free multimedia in everyday life*
3. *Engaging in citizenship through digital technologies*
4. *Citizen journalism, Sharing stories in digital world*

Lesson 1

–

Digital identity and mobile media

Every interaction taking place in a digital environment provides data on what the user's activity in that environment, playing a role in personalisation, destination marketing, digital reputation, social media and graphical services. In other words, the digital footprint left is as large as the number of people or entities we interact with online. Module 1 contains lesson 4, the topic of which is precisely the digital footprint, a concept directly related to digital identity. As an introduction to this lesson, learners can be reminded of the concepts associated with a digital footprint by using the multimedia quizzes assigned to lesson 4, module 1.

A digital identity can be defined as all online information and data about a specific person and consists of information/data such as:

- *Authentication elements: email address, username, password, surname, first name, IP address, etc.*
- *Personal, administrative, professional, banking, social data, etc.*
- *Identifiers: photographs, logo, image, avatar, etc.*
- *Digital footprints: using social media, writing a blog, commenting some online content, etc.*

The aims of the first lesson of this module are to understand the importance of personal data and the role of mobile media in producing and organising it, and how to acquire and effectively use software dedicated to organising personal data.

.

MODULE	Active participation in the information society	LESSON UNIT	1	TOPIC	**Digital identity and mobile media.** Use of self-measuring and data producing mobile devices and applications to build digital identity.

LEARNING OUTCOMES:

- Learners will understand the value of personal data and role of mobile media in producing it.
- Learners will know how to use mobile media sensors to gather and manage personal data.
- Learners will know how to acquire and use software dedicated to organise personal data.
- Learners will know how to organise data flows to get required personal goals with data.

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY: "Quantified self" (time: 15 mins)	To make learners familiar with the general idea of the lesson and its agenda.	The trainer synthetically presents a case study in the form of the "Quantified self" project and: - explains the socio-cultural meaning of the project, pointing to the contexts of network data circulation, mechanisms of electronic supervision and social control; - indicates the techniques used in the project: the applications and tools used (smartphone, smartwatch, notebook, sports band), refers to their modern versions and the possibilities they offer to their users; - discusses the possibilities of digitizing data for one's own needs based on a case study and at the same time reaches for additional possibilities beyond the analysed material.	• projector & computer

TRY TO NAME: sensors and data flows naming and mapping (time: 25 mins)	To recognise the hardware capabilities of mobile media in the field of acquiring personal data and to characterise of this type of data	1. The trainer indicates and names the most popular sensors available in smartphones. For this purpose, s/he uses one of the popular applications that allow to recognise the capabilities of mobile devices and read the operation of sensors in real time - e.g.: for Android and iOS these will be: Sensors Multitool, SensorLab, and My Device. 2. Learners install the applications selected by the trainer to create a list of sensors available in their smartphones and mobile devices. (Other mobile devices paired with a smartphone can be analysed in the same way). 3. Each learner creates their own list of sensors that can be used, associating them with data that they can and want to source for further analysis. (here the matter of a quiz)	• projector & computer, Internet access, smartphones - multimedia: - an info-graphic of smartphone sensors and its capacities and connections - interactive quizzie associating selected sensors with possible data streams
ACT: **combining sensors and data with apps** **(time: 25 mins)**	To connect personal data with applications for their organisation and use	1. The trainer presents the selected applications that allow for automated, personalised analysis of data from sensors in the smartphone and connected peripherals. * (List of applications for personal data analysis). 2. Depending on their preferences and needs, each learner installs selected applications and begins the collection and preliminary analysis of data gathered in this way. 3. Learners try to work with data and applications in such a way as to prepare a short summary of this type of activity and present it to the rest of the class at the end of the lesson. Here you can follow the answers to the questions about data that learners want to share, which they do not wish to share, which they should, and which data should be purely private.	• projector & computer, Internet access, smartphones

GOOD PRACTICES **Sharing experiences and discussion.** **(time: 17 mins)**	To compare the possibilities of activities and to discuss the achieved results	1. The trainer invites learners to share the effects of their work and arranges a discussion around them. 2. The trainer presents additional examples and good practices that have not appeared during the lesson, expanding the field of possible activities in the future.	
SUMMARY, feedback (time: 8 mins)	To summarise the lesson	The lecturer summarises the current lesson referring to other lessons and modules as well as quizzes and multimedia materials available under the project.	

Quiz 1

This is a quiz designed to be used during learner activities. It shows what sensors can be found in smartphones and the possibilities for their use. In the 'Naming' stage of the activity, which is about sensors and data flow, the trainer displays the quiz to the learners and they try to come up with the possibilities there are for using a particular sensor. A table with the sensors listed in the quiz is presented below:

Sensor	Its use
sensors of available cameras	photos, video transmissions, films, biometrics
GPS	location, routes, movement history
Accelerometer	movement, acceleration, mobility
Gyroscope	ways of the device application
Magnetometer	orientation relative to magnetic poles
Light sensor	Responses to ambient light
Microphones	acoustic signals
Proximity sensor	proximity of device to body
Pedometer	body activity
Thermometer	temperature changes
Humidity sensor	changes in air humidity
Pressure sensor	changes in atmospheric pressure
Fingerprint sensor	biometrics
Touchscreen	touch modes, biometrics
Wi-Fi	accurate location, monitoring transfers and connections
Bluetooth	monitoring transfers and connections

Quiz 2

This quiz, like the first one, is for use at the same stage of the lesson. It is a multiple-choice quiz to allow learners to test their knowledge. It consists of identifying the correct data acquisition opportunities according to the indicated sensors. The learner's task is to click on the respective sensor and select the data acquisition opportunities for which the sensor is responsible. Below a table with the sensors used in the quiz and the correct answers (marked with a plus) are given.

- **Available camera matrices**
  1. Biometric patterns +
  2. Behavioural patterns +
  3. Visual information regarding places +

- **GPS**
  1. Health condition -
  2. Current geographical location +
  3. Daily activities +

- **Accelerometer**
  1. Movement coordination in X, Y, Z dimensions +
  2. Mobility patterns +
  3. Periods of movement and rest +

- **Gyroscope**
  1. Behavioural patterns +
  2. Shopping preferences -
  3. Biometric data +

- **Magnetometer**
  1. Biometric data -
  2. Shopping preferences -
  3. Mobility +

- **Light sensor**
  1. Behavioural patterns +
  2. Social interactions +
  3. Mobility -

- **Microphones**
  1. Knowledge on social interactions +
  2. Biometric profiling +
  3. Behavioural profiling +

- **Proximity sensor**
  1. Daily activities +
  2. Shopping preferences -
  3. Biometric profiling -

- **Pedometer**
  1. Daily activities +
  2. Behavioural patterns +
  3. Lifestyle +

- **Thermometer**
  1. Location data +
  2. Biometric profiling -
  3. Shopping preferences -

- **Humidity sensor**
  1. Shopping preferences -
  2. Biometric profiling -
  3. Environmental data +

- **Air pressure sensor**
  1. Shopping preferences -
  2. Biometric profiling -
  3. Environmental data +

- **Fingerprint sensor**
  1. Biometric profiling +
  2. Shopping preferences -
  3. Interactive daily activities +

- **Touch screen**
  1. Interactive daily activities +
  2. Knowledge on social interactions -
  3. Behavioural patterns +

- **Wi-Fi**
  1. Number and names of wireless networks in the immediate vicinity +
  2. Position towards neighbouring Wi-Fi routers +
  3. Audio and video recordings -

- **Bluetooth**
  1. Social interactions +
  2. Data transfers +
  3. Monitoring of peripheral devices +

Lesson 2

-

Remix – free multimedia in everyday life

Traditional methods of searching for information of interest online are based on browsing the World Wide Web. It is important to remember that the Internet is not only about websites, but is full of different search engines, directories, databases and other services that allow its users to search for information and resources of various kinds. However, when searching for material on the web, it is important to remember that only a small part of it can be used freely. It is important to check beforehand under what conditions the material has been made available.

In the initial stages of the lesson, the trainer can explain to the learners that open resources are materials that are made universally accessible, free of charge for use and available for use under an open licence. Open resources can take the form of written and spoken texts, images, radio and TV recordings, animations and other videos, tests, quizzes or games, or source codes.

The lesson aims to familiarise learners with the concept of open resources. They will learn where to look for free multimedia, what to be aware of when using works found on the web, and the essential role of open and free multimedia resources.

The lesson topic uses the word 'remix'. The term may be associated with music, but here it is used as a technique that may be used in the creation of various materials. Remixing involves taking already existing pieces of work (music, film, graphics, etc.) and combining them in such a way that an entirely new work is already created. The use of any photo editing software, with which one can rework a photograph in a way one has imagined and thus create a new image is an example of this phenomenon.

MODULE	Active participation in the information society	LESSON UNIT	2	TOPIC	**Remix – how to get and use free multimedia in everyday life.** Searching and using open multimedia content for personal use

LEARNING OUTCOMES:

- Learners will become familiar with the search options for multimedia information resources.
- Learners will know the most popular open media websites.
- Learners will understand the cultural role of open and free multimedia resources.

STAGES	AIMS	PROCEDURE	ZASOBY
CASE STUDY: **art masterpieces downloaded, remixed and printed for your wall or t-shirt!** **(time: 20 mins)**	To present exemplary possibilities of obtaining legal, free-to-use multimedia resources available on the Internet.	The trainer presents the possibilities of searching selected websites offering free and open multimedia resources as an alternative to purchasing files at file stocks and pirated resources. As an introduction to the case, trainer uses the Rembrandt Remix project offered by the Rijskmuseum. In this context, s/he introduces learners to the availability and circulation of multi-media resources on the Internet, first of all emphasising such circulations and environments that are of open and social nature. Trainer: • indicates websites and services that offer multimedia for free use: movies, music, photos, drawings, templates (MULTIMEDIA: an infographic presenting selected sources of legal, open multimedia resources) • presents selected projects implemented with the use of free, social multimedia	• projector & computer • MULTIMEDIA: - an infographic presenting selected sources of legal, open multimedia resources - an infographic showing the stages of the process from

		• briefly reminds about the possibility of collecting multimedia in the form of an online collection as well as the possibility of downloading selected resources to one's own digital devices in the form of files. (MULTIMEDIA: an infographic showing the stages of the process from searching to using multimedia material)	searching to using multimedia material
TRY TO NAME: **Following keywords, topics and data structures.** **(time: 25 mins)**	To recognise possible techniques of navigating among internet databases that contain multimedia materials.	The trainer divides the learners into pairs. Their task will be to select one of the previously indicated open database containing multimedia and navigate in it according to the technique indicated by the trainer. Learners can choose techniques based on the use of keywords, timelines, technical format of the searched materials (photos, recordings, clips, articles), or authorship. Individual groups are asked to test selected techniques in order to explain the possibilities that were achieved thanks to them within individual multimedia databases. Each group performs this task in relation to 1-2 websites (e.g.: the group first searches the general Europeana.eu resources using the *oriental plants* tag. Then, in the same way, the group searches for resources in a national museum of their choice, in the collection of a scientific institution, a specialised blog or a photo service).	• Computers with the access to the Internet
ACT: **Build your own free multimedia collection.** **(time: 25 mins)**	To search and collect multimedia materials for one's own needs.	Learners try to work on their own with multimedia. They search, collect and pre-catalogue multimedia materials from various open and legal sources for their own needs. To this end, they indicate their own keywords, establish technical needs and make an initial selection of previously known websites and look for additional ones offering the necessary materials.	• Computers

		The collection created in this manner may assume the form of a list of direct links to specific files, or a catalogue of these files stored in the computer memory.	
GOOD PRACTICES **Sharing experiences and discussion.** **(time: 15 mins)**	To present the results of one's own research, advantages and disadvantages of the adopted solutions, and to conduct a summarising discussion.	Each learner explains their way and outcomes achieved focusing on selected resources. The trainer is wrapping-up the lesson topic and its outcomes trying to point at the pros and cons of presented strategies. Learners are welcome to comment and to share their own good practices.	
SUMMARY & FEEDBACK **(time: 5 mins)**	To summarise	The trainer summarises the classes, referring to other lessons and modules as well as to quizzes and multimedia materials available under the project.	

Two quizzes are planned for this lesson as well, both of which will be necessary for the case study provided in this lesson.

Quiz 1

The quiz collects links to various free web resources. The user clicks on each category and is presented with free sites that provide content from the given categories.

category	resources
Creators	The most numerous but also the most dispersed resources are those created and made available by individual creators. These can be found, for example, on sites that collect and promote their work. jamendo.com, Flickr.com, medium.com
Communities	An important role in finding relevant resources can be played by fan communities, who browse online sources, index the resources available in them and curate them both for themselves and for others. Thenounproject.com, openculture.com, deviantart.com
Institutions	An increasing number of cultural, arts, media and digital institutions are choosing to make their collections digitally available on an open access basis. www.metmuseum.org, www.europeana.eu
images	Flickr.com, Thenounproject.com, pixabay.com
films	pexels.com, vimeo.com, adobe.com
sounds	jamendo.com, soundcloud.com, spotify.com
texts	openlibrary.org, otwartelektury.pl, www.gutenberg.org

Quiz 2

This is a quiz entitled "From the need to the remix – how to find and use open multimedia resources" and it is an interactive infographic outlining how to source free, open and legal multimedia resources. The next steps are presented in the form of icons, and the user clicks on them on the screen to move to the next stages of the exercise. Quiz content:

1. *An idea – do you have an idea for your own video, proclamation, multimedia presentation, audio clip, playlist, an article or other simple multimedia projects? You can prepare them based on materials you buy from image, clip and content banks, or try to do the same using legal resources and templates available on the web for free based on various licenses.*

2. *A need – perhaps you need photos, songs, video clips, or vector graphics material. Such resources can be easily obtained from the creators themselves, from open institutions or with the help of fan communities. If you know what you are looking for, the list of specialist services is very long.*

3. *Research –collect, tag and organise resources for your own use. When collecting materials, make sure you choose materials that are free of financial obligation. Take the opportunity to find out about legal licenses alternative to the dominant ones that determine the possibilities of using the resources – Learn about Creative Commons licenses — Creative Commons Polska.*

4. *Production – you can use more than just open and free multimedia resources to edit your content. You should also use software and digital services for producing multimedia content for free. Most of the expensive and complicated commercial programmes have their free, open-source equivalents. See for starters – Top 10 Free Alternatives to Expensive Software (lifehacker.com)*

5. *Publication and dissemination – also in terms of putting your completed content online and attracting viewers to it, it is worth using alternatives to paid options. You can always place your work on those free portals and services you used during the research stage. In this way you will give back to the community what you have gained thanks to it. See for starters – Top 10 Free Alternatives to Expensive Software (lifehacker.com), 10 Best Free Video Hosting Sites for Private/Business Online (wondershare.com)*

6. *Feedback synergies – you can count on someone being interested in your work. As a result, it will start to enter the digital world and spread its influence. Perhaps it won't happen immediately and the reach won't be great at the beginning, but certainly the reactions to its presence in the global information flow network will give you interesting feedback on what you have done and how you have done it.*

Lesson 3

–

Engaging in citizenship through digital technologies

Virtual reality is an integral part of modern life. It is not just about the time spent in front of a computer screen, but it is also in front of phone screens and even watches. In this way, the digital world is merging with the real one. The way civil society is being built and developed is also changing. The necessary civic skills in the information society rely heavily on media skills and practical technical competences.

Electronic media are changing the way people communicate. Online communication complements traditional interactions, with social media in particular providing opportunities to reach a wide range of internet users. Social networks and electronic media equip citizens and institutions with a variety of tools to share information and organise themselves. They provide a means by which each person can voice his or her own opinion, protest, and thus contribute to increasing citizen involvement in social, administrative or political matters.

Many Internet users participate in various online services or use diverse online tools (forums, chat rooms, groups, instant messaging, online games). This puts them in contact with other Internet users and creates a community based on shared characteristics such as interests, political views, work, social or health problems.

Thanks to this lesson, the learners will learn about the possibilities to engage in various civic activities through digital technologies, understand the role and importance of activist projects conducted in the digital environment and be able to critically interpret activities in the digital media environment.

MODULE	Active participation in the information society	LESSON UNIT	3	TOPIC	**Engaging in citizenship through digital technologies** Engaging in civic activities through digital technologies

LEARNING OUTCOMES:

- Learners will be familiarised with various possibilities of engaging in civic activities through digital technologies.
- Learners understand the role and importance of activist projects carried out in the digital environment.

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY: **civic activities in the digital world** **(time: 20 mins)**	Presentation and discussion of the concept of a civic activity implemented with the use of digital technologies. Making reference to the idea of digital citizenship and a preliminary analysis of selected examples.	The trainer introduces the subject of digital citizenship referring to the categories of digital revolution, civil society, electronic public sphere, open state and democracy. In this context, the trainer indicates the existing civic activities and projects undertaken by civil society with the use of digital technologies and social networking sites. Social generation, processing and use of data- place memory and historical resources, civic activism, monitoring of infrastructure activities.	• projector & computer MULTIMEDIA: a compilation of iconic, successful and unsuccessful social actions carried out in the digital environment MULTIMEDIA: infographics presenting the directions of civic engagement through digital media and the web

TRY TO NAME: **Forms of digital engagement and ways of designing civic actions.** **(time: 20 mins)**	Discussion of the possibilities and limitations related to the use of various forms of involvement in digital activism. Overview of functional methods of operation: apps, information exchange formats as well as existing standards for the circulation of information and data.	The trainer divides the learners into teams of three. The task for each of the teams is to attempt an in-depth analysis of one example from those previously discussed. The learners are to write down the sequence of activities undertaken in the discussed project and assess the effectiveness of the selection of specific tools, formulas, and rules of communication. Important elements to be taken into account here include the activity coverage and building network communities and inclusive relationships around them, using various communication channels and available digital resources - multimedia, data, public and commercial websites and services, as well as generating them.	• Computers with access to the Internet
ACT: **Design civic activity plan to help communicating a local problem and build social network around it.** **(time: 30 mins)**	Designing civic activities in a digital environment.	The learners will face the challenge of designing a general outline for possible communication activities in the digital environment. In groups of several people sharing common interests, idea or needs, they will attempt to devise a scenario for an action aimed to publicise the problem, build network communities and a forum for exchanging opinions around it, collect the necessary digital resources - multimedia, apps and data.	• Computers
GOOD PRACTICES **Sharing experiences and discussion.** **(time: 15 mins)**	Presentation of the results of the project work and a follow-up discussion.	Each classmate explains their way and outcomes achieved focusing on selected resources. Trainer is wrapping-up the lesson topic and its outcomes trying to point at the pros and cons of presented strategies. Learners are welcome to comment and to share their own good practices.	

In the first stage of the lesson, i.e. a case study, the use of two multimedia quizzes is planned.

Quiz 1

What can we do together with the use of media? A quiz that compiles various successful and unsuccessful social actions implemented in a networked environment. While user clicks on the icons, the quiz shows both actions in several categories and their corresponding examples:

Blockchain – one of the most popular ways of operating in networks both outside corporations and state supervision. Each member of some online community authenticates events in this network by noting their existence and storing them in the form of a digital certificate. The blockchain rule has been used to create circulating digital currencies (Bitcoin), digital certificates of uniqueness (NTF) or to confirm digital identities (digital identity).

Applications – people collaborate with one another through electronic media not only to solve current problems. Many of them are involved in projects that result in tools for others based on the logic of open code and easy availability and in most cases also remain free for the average, non-business user. Examples: LibreOffice, a free office application suite, Firefox an open web browser, or SETI@home, a volunteer search for extraterrestrial life.

Databases – also data collection and organisation on the basis of the common good bring very tangible effects. There are numerous examples of citizen involvement in projects aimed at building and sharing databases dedicated to different fields of knowledge. Examples: OpenStreetMap or map of the world, or many projects from the wiki family, such as WikiMedia dedicated to collecting educational resources.

Crowdsourcing – i.e. community financing of selected initiatives, activities or organisations via applications or websites. In this way, citizens can directly co-finance necessary and, in their opinion, valuable events. Examples (with record funding): a series about the life of Jesus (The Chosen), or a community project related to remembrance of the war (Europeana 1914–1918).

Forums and discussion groups – one of the most well-known and common forms of civic activity involving digital media. For many users of these media it is still the most acceptable and convenient form of engagement. Examples: Ushahidi – an application and platform for collaboration in case of crisis events, or OpenIDEO for exchanging views and shaping ideas together.

Grassroots journalism – journalists and media often unable to do the necessary research work themselves. Frequently media institutions fail to cover topics due to various constraints, interests and political games. This is an excellent field for amateur journalists and community media projects. Examples: community collaboration on journalistic investigation material (Guardian), or a local newspaper edited and published by the local community (Fitzrovia News).

Quiz 2

Before showing this quiz, depending on the group of learners and the time allocated in the lesson, the trainer may ask the learners about their experiences of online civic engagement and directions for its development. This quiz can be taken as a summary of the discussion that will emerge between the learners. It shows different directions for civic engagement using digital media and networks. These are not all possible directions, but only examples of them. Learners may feel welcome to add their ideas.

Local communities – strengthening bonds, grassroots projects, citizen monitoring

Scattered communities – collaboration across time and space, circles of influence, articulation of ideas

Political activism – controlling political elites, exchange of ideas, software and e-services

Citizen journalism – beyond the mainstream, local debate, community collaboration

Data collection – open databases, social control of data, collective memory

Lesson 4

–

Citizen journalism. Sharing stories in digital world

Citizen journalism can be understood as a type of journalism practised by non-professional journalists in the public interest. Most often, this activity is linked to the development of the Internet and, in particular, to the emergence of online news sites whose content is created or co-created by Internet users. Various forms of citizen journalism are now possible, e.g. these may be posting texts or images on one's own news sites or on existing platforms, or writing a blog.

The aim of this lesson is to explore the basic conditions for creating and publishing information in a digital environment, to understand the opportunities and constraints that arise at the various stages of communicating information projects in a digital environment, and to acquire the skills necessary to select tools appropriate to the digital environment.

The trainer should pay particular attention to certain aspects of citizen journalism, which always involves responsibility for the content published. The content must be truthful, reliable and verified. Although every text contains the author's point of view and therefore is subjective, it is nevertheless necessary to be honest with the people described. Citizen journalists are also responsible for the impact they will have with their text. One must be aware of the possible consequences of publishing a test. Even if all the information provided is verified and fairly captured, its publication can sometimes have negative consequences, which should be anticipated by the author of such a text.

Citizen journalism brings together various activities, such as exposing or highlighting problems in the local community, writing reports on interesting and unknown events and places, describing interesting characters, and writing journalistic or popular science texts.

MODULE	Active participation in the information society	LESSON UNIT	4	TOPIC	**Citizen journalism- sharing stories in digital world** Basic communication tools and rules for citizen journalism.

LEARNING OUTCOMES:

- Learners will know the basic conditions for creating and publishing information in the digital environment.
- Learners will understand the possibilities and limitations that arise at the different stages of communication of information projects in the digital environment.
- Learners will be able to choose a set of tool appropriate to the digital environment.

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY: **Citizen journalism: ideas, tools, practices** **(time: 20 mins)**	Presentation of the idea of civic journalism and discussion of information circulation in digital conditions.	The trainer introduces the subject of civic journalism, pointing to the differences with the operation of professional media institutions, disadvantages and the advantages of this model of operation and presenting the most famous examples in this area. The trainer goes on to discuss a possible workshop for a citizen journalist, pointing to tools and platforms for working on content, making it available in the network circulation and building an environmental base for it. In the introduction, the trainer refers to such categories as public debate, reporting, collecting information, information research and open data as well as collaborative journalism.	• projector & computer MULTIMEDIA: infographics demonstrating the stages ranging from collecting data, through designing information to introducing it into the network circulation and building a social media reach for it MULTIMEDIA: infographics presenting a collection of the most popular, accessible tools for citizen journalism

TRY TO NAME: **Stages of designing and communicating journalistic content in a digital environment.** **(time: 20 mins)**	The specificity of tasks and stages of citizen journalists' work based on the analysis of case studies.	The trainer divides the learners into three teams. The task of each team will be to identify the components of each stage of the content flow, its requirements and limitations. The learners are asked to write down the sequence of activities undertaken in three individual stages of the indicated projects- case studies and to evaluate the effectiveness of the selection of specific tools, formulas, and rules of communication. The first team will deal with the stage of gathering information and structuring the message - the methods and conditions of acquiring knowledge, checking the credibility and usefulness of information, creating simple media messages. The second team will focus on the possibilities of disseminating civic information and analyse media platforms for information distribution as well as indicate the channels that are the most effective in specific cases. The third team is to analyse the communication effectiveness of selected journalistic strategies. Team members will try to answer questions concerning how many recipients they have reached and how successfully the selected content has been disseminated. Has there been a change in the state of affairs thanks to it?	• Computers with the access to the Internet
ACT: **We design a bottom-up information event.** **(time: 30 mins)**	Designing a comprehensive scenario of an action in the spirit of civic journalism.	Divided into two groups, the learners will face the challenge of creating a general scenario aimed at disseminating the content in a digital environment. In the discussion, the group identifies a problem that requires publicity in the network environment and tries to choose the most appropriate ways of proceeding at particular stages of its communication. As a result of	• Computers

		this reflection, a scenario is created that defines the general rules of operation, necessary tools, duration, expenditure and the necessary resources.	
Summary and discussion (time: 15 mins)	Discussion summarising the results of the project work.	The groups present the assumptions of their scenarios and together analyse their advantages and disadvantages.	
Summary and feedback (time: 5 mins)	Summary	The trainer summarises the lesson referring to other lessons and modules as well as quizzes and multimedia materials available under the project.	

Two multimedia resources are provided for this lesson too, which are for use at the case study stage.

Quiz 1

This quiz demonstrates the stages from idea to implementation. It is designed to be used in class, but thanks to making all the material available on the platform, learners can return to it at any time. The quiz can be displayed on the interactive whiteboard or each learner can do it independently. It includes the stages of work for creating materials in citizen journalism. Learners click on the names of the stages and familiarise themselves with their role.

Message – The most important thing is what you want to say; ideally if you have a precise topic, interesting information to convey and you want to convince a specific audience to your point of view. Think about the information you want to convey and the story form you will adapt. You will need a script, data in graphical form, and graphic material such as photos, icons, and charts.

Research – You already know what you want to say and what to convince your audience of. The story must be documented and based on reliable sources. Do your research: find the necessary data and information, organise them and arrange the points in the scenario based on them. Note down the sources carefully – write them down in the content of the infographic so that the viewers can access them.

Format – Give your work a story form. Use factual arguments supported by data and illustrations that are logically connected. Start the story with a title and a short description, which can take the form of a question. Finally, summarise your story, draw conclusions and encourage discussion.

Layout – An infographic can be more pictorial or more textual or have more or less iconic elements, charts, and styling. Match the visual profile to the meaning of the story – it can be more artistic or more 'tabular' depending on the overtone and reception you wish to achieve. You can use ready-made templates offered by many portals.

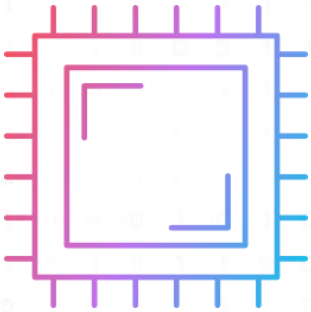
Publication – For your work to gain an audience, it needs the right distribution channels. Use social media, media platforms as well as print or forms of direct communication. Having planned your target audience beforehand, try to reach them and show them what you have done.

Range – Be sure to get the right reach for your work. Initiate discussions around it, get people to comment and forward it on. The more that happens around it, the more people will see the infographic and you will learn a lot about its perception, environmental reactions and manners in which it can be used.

Quiz 2

It collects links to online tools that can be helpful for content creation within citizen journalism. The trainer can remind the learners that all the multimedia that appear in the class are available on the platform and any learner can access it at any time. In the quiz there are links to the tools in question, divided into thematic categories. Of course, these are not all the possible tools available on the web, but only some examples. The trainer can expand the tool portfolio if they are aware of any interesting and helpful sites. Below the table presents the examples used in the quiz.

category	tool
Photos	taking photos: Google Camera, Open Camera, filming: FiLMiC Pro, ProCam X, scanning: Adobe Scan, Office Lens, processing: Adobe Photoshop Express, GIMP, organisation: Adobe Bridge, FastStone Image Viewer, photo banks: Pixabay, pexels
Sound	recording and editing: audacityteam, publishing: souncloud, spotify
Text	Google Docs, Libre Office, WordPress
Information	Feedly, Pocket, Slack
Data	Tableau Desktop, Datawrapper
Visualisations	canva, infogram, visme
Infographics	visual.ly, piktochart



MODULE 4
–
CONSCIOUS USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

A myriad of information can be found on the web. However, it may not always be of great value. It is a well-known fact that the possibilities of controlling content on the Internet are definitely limited. Various portals may publish information, but it depends on the user's decision whether they consider it to be reliable and coming from a reliable source or it is deemed to be useless and untrue. In cyberspace, publications are monitored and commented on by internet users themselves. Comments on and criticism of posted content are not always objective, as anyone can express themselves online. For this reason, the lessons in this module are oriented towards a critical approach to online material and equipping learners in the 'iAware' programme with the ability to verify the content of a website and the correctness of the information it contains.

Module four includes topics such as:

1. ***Fake news***
2. ***Media literacy – how to detect fake news?***
3. ***Disinformation and misinformation***
4. ***Conscious use of ICT***

Lesson 1

-

Fake news

This lesson focuses on the concept of 'fake news', i.e. in English-- simply false information. It is content that is untrue or not entirely true, but is nevertheless published on news websites or social networks. It is not always published in text form, but can also use graphics, images and even videos in which the content is manipulated through processing.

Fake news is part of a wider internet phenomenon of reality and image falsification. It created and disseminated, for example, for political or financial reasons and can also be created for entertainment purposes to, among other things, draw attention to the medium or person promoting it.

Fake news can be disguised as real information, media articles or even scientific content. Sometimes it appears as tweets published by people who do not exist, as well as internet memes or propaganda texts. What these forms of fake news have in common is that they are intended to mislead the audience. Fake news can be disseminated immediately with this intention, but very often it is passed on through people who believe in its content.

The first lesson is aimed at preparing the learners to be critical of information appearing on the Internet, to acquire the ability to recognise fake news and different news sources, and to understand the dangers of it.

MODULE:	LESSON UNIT:	TOPIC:
Types and identification of Fake News		Fake News
catiaalvescruz@gmail.com		
Cátia Cruz		

LEARNING OUTCOMES:

- Learners will understand the different sources of news
- Learners will understand the value of being well informed and the danger of fake news
- Learners will be able to identify fake news

STAGES	AIMS	PROCEDURE	RESOURCES
CASE STUDY: **"O arrastão de Carcavelos"** **(time: 10 mins)**	To acquaint learners with the goals and results of the training To familiarise learners with an example of fake news before digital era	1. The trainer greets the learners and acquaints with the lesson plan and its successive stages 2. The trainer synthetically presents a famous case study that happened in Portugal in 2005 and will introduce: Trust, Truth and Journalism	• Projector & Computer
Task **Introduction to Fake News** **(time: 10 mins)**	Introduce what fake news mean and familiarise the learners where "news" come from	The learners will watch a video that will introduce these topics: • News information transformation: Digital technology, Social Platforms and spread of fake news • The phenomenon of "information disorder": formats of Misinformation, Disinformation and Mal-information.	• Projector & Computer

Task **Effects of Media Misinformation (time: 15 mins)**	To familiarise the learners with the importance of being well informed and the consequences of fake news	1. The trainer introduces the learners to the remaining activities of the lesson. Based on the previous lesson stage, the trainer describes the most famous types of fake news and how it spreads nowadays. 2. The trainer talks to the learners about Social media, try to understand if they check news before sharing and if they ever reported to Facebook a fake news. 3. The trainer interacts with learners and try to understand how do they think we should combat disinformation and misinformation 4. The trainer shows a video with a practice example on the critical ability to deconstruct fake news. 5. The learners answer the trainer's questions and share their reflections on the watched video.	• a projector and computer with internet access for the trainer •
Task **How to identify Fake News (time: 25 mins)**	To understand how to verify and identify Fake News The learners together will access to news sources and visual content and do an exercise of fact-checking and Social Media Verification	1. The trainer explains how to identify a trustful source of news 2. The trainer asks the learners to think about content they have read in the past week and which they think are fake news 3. The learner's task will be to classify and divide which news will be presented and the one´s they believe are truth or fake: • Newspapers well established in Portugal • News from online blogs • News shared on Social Media • Examples of facts that are told from Politicians in interviews With the support of the trainer the learners will verify if the news is fake.	• a projector and computer with internet access for the trainer • work with computers- learners have access to a computer with the Internet connection Sources: • Websites • YouTube videos • Social Media • Search Engines

GOOD PRACTICES (time: 10 mins)	Together with the trainer learners will be divided in groups and create news	1. The learners will produce news. Colleagues will have to identify which are true and which are not.	• a projector and computer with internet access for the trainer and learners •
FEEDBACK/ REFLECTION TASK (time: 5 mins)	To revise and verify the acquired knowledge. To obtain feedback from learners regarding the lesson.	The trainer summarises the lesson and checks learner's reaction to the lesson (positive / negative). Learners will receive a winner batch saying "You don`t fool me, I`m a fact checker"	

The trainer should explain to the learners that fake news is not only spread through social media, but can also be found in traditional media. People are used to associating fake news with the internet and social media, yet fake material has previously spread and continues to spread via traditional media too. Paradoxically, providing false information in a traditional newspaper or television reinforces it many times and it spreads with reference to that source.

A tailored educational materials are created for this lesson plan in the form of videos and interactive quizzes. All multimedia materials are available on the 'iAware' programme platform in the trainer and learner sections.

Quiz 1

An interactive quiz that can be displayed on the screen and taken during the lesson, or learners may be requested to take it themselves after the lesson. It is a test of the knowledge that learners should have after covering the topic of the lesson. It consists of questions with one correct answer, which should be chosen by the learner.

1. *How is fake news defined? What characteristics might it have?*

    a. Disinformation

    b. Lack of information

    c. Misinformation

    d. All of the above (correct)

2. *Can a rumour be a form of fake news?*

    a. Yes (correct)

    b. No

3. *If a broadcaster in the traditional media begins to distort a story to gain an audience, can this be considered a falsification of reality?*

    a. Yes (correct)

    b. No

4. *Fake news aims to:*

   a. deceive and manipulate (correctly)

   b. manipulate and request

   c. communicate

   d. all of the above

Quiz 2

Similarly to quiz 1, it can be used in a lesson or during the learner's independent work. It consists of a number of questions where one correct answer from four possible ones must be marked. The quiz can be viewed as a verification of the learners' understanding of the lesson material. Below the content with the correct answers is presented.

1. *A fake News has the following characteristics*

   a) Be like a virus

   b) It is easily propagated

   c) It can easily be taken for granted

   d) All of the above (Correct)

2. *What are the stages of Information Disorder?*

   a) Creation, Production and Distribution (Correct)

   b) Preparation, Production and Launch

   c) Production and Distribution

   d) All Previous

3. *What are the Diffusion Stages?*

   a) Create a Blog; Write Content; Sell Advertising; Disclose by SMS; Repeat.

   b) Create a fake news site; Steal Content; Sell Advertising; Publish on Social Networks; Repeat. (Correct)

   c) Write Content; Sell Advertising; Disclosure via the Website; Repeat.

Lesson 2
–
Media literacy – how to detect fake news?

Using this lesson, students will learn the concept of media literacy and its role in the context of fake news. They will also acquire skills on how to identify fake news and what tools can be used to do so.

Media literacy can be understood as the training of competences for an informed use of the media, based on knowledge, attitudes, motivations and skills, in which users are able to interpret the meaning of messages and understand how messages or media content are constructed as well as be familiar with the consequences of disseminating unverified information. Media literacy is not only the ability to use the internet and mobile devices, but above all the ability to use the media appropriately and consciously. A media literate person should be able to distinguish between a valuable, accurate message and one that is intended to provoke emotions, fear, prejudice or spread untruths.

There is no one-hundred-percent effective method to identify fake news. There are many clues that can arouse and increase suspicion of deception. This lesson will help in learning to recognise false information. However, the trainer must make the learners aware of the fact that the acquisition of media skills cannot be of a one-off nature. The world of media, information, and new technologies is changing so fast that continuous media education and ongoing media literacy is needed.

MODULE:	LESSON UNIT: 1	TOPIC:
Media Literacy - How to detect fake news		Media Literacy - How to detect fake news

LEARNING OUTCOMES:

- What is Media Literacy
- Understand the role of Media Literacy in the context of Fake News
- How to spot fake news
- Tools to detect and debunk fake news
- Develop Media and Information Literacy Skills

STAGES	AIMS	PROCEDURE	RESOURCES
Introduction to Media Literacy	• introduce the concept of Media Literacy	• The trainer introduces himself • The trainer introduces the main concept of Media Literacy using a power point • The trainer ask students about their understanding of media literacy • The trainer introduces the concept of Critical Thinking • The trainer gives examples of the linkage between Media Literacy and Critical Thinking	• Projector and Internet access
Task (duration: 15 mins)	• Developing a word map for the main concepts of media literacy	• The trainer presents the task • The task is to identify the main concepts about media literacy that are found through a web search • Each group build there own word cloud • Each group presents the results to the class	• Projector and Internet access • Computer for students

		• The trainer promoves a discussion about the results so students can look and compare their results with the ones found other students groups	
How to spot fake news	• Give students skills on how to detect fake news	• The trainer presents several techniques about detecting fake news • Students watch a video from YouTube about fake news https://www.youtube.com/watch?v=Q8su4chuU3M&ab_channel=TheFrance24Observers • The trainer gives examples for each one of the steps for checking fake news • The trainer explores the different media content present in a news that should be critically evaluated	• Projector and Internet access • Computer for students
Task (duration: 25 mins)	• Give students practical insight in identifying fake news by the use of a critical approach	• The trainer presents 3 headlines and text and media content • The student's task is to identify if the news are fake or not following the steps identified in the previous lesson • The students share the results and details the reasons for their conclusions	• Projector and Internet access
Good Practices (duration: 10 mins)	• How to deal with fake news in our daily live	• The trainer wraps up the the main concepts discussed during the lesson • The trainer asks students to share their own conclusions about the role of media literacy	
FEEDBACK/ Active reflection (duration: 5 mins)	• Critical reflection about fake news and there impact for democracy and citizenship	• The trainer deliveres to the students fake news examples • The trainer asks students to think about the implications for society if people take them as truth. • General discussion among teacher and students • The trainer ends the session giving a general overview of it	

There are two interactive quizzes for this lesson, which can be used in class or the learners may be asked to do them themselves. The quiz is a summary of the lesson and a test of knowledge regarding fake news. The quizzes are available on the 'iAware' platform.

Quiz 1

This is a multiple-choice quiz. The task of the person doing it is to mark all possible correct answers in each question. Below the content of the quiz is given.

1. *What is Media Literacy?*

   a) Practices that allow people to access, critically evaluate, and create or manipulate media.

   b) A set of essential skills for work, life and citizenship.

   c) It is intended to promote awareness of media influence and create an active stance towards media consumption and creation.

   d) All of the above (Correct)

2. *Is Thinking Organized and Rational One of the Characteristics of Critical Thinking?*

   a) Yes (Correct)

   b) No

3. *Select some of the important skills for critical thinking.*

   a) Analysis (Correct)

   b) Interpretation (Correct)

   c) Evaluation (Correct)

   d) Explanation (Correct)

   e) Attention

   f) Open Mindedness (Correct)

   g) Problem Solving (Correct)

Quiz 2

Similarly to the first quiz for this lesson, this is a quiz with more than one correct answer. The learner marks all the correct answers on the screen. Below the questions that appear in the quiz with the correct answers marked are presented.

1. *What should we pay attention to when we read the news?*

   a) Read beyond the title

   b) Check the author

   c) Check support sources

   d) Check date

   e) Check if it's a joke

   f) All of the above (Correct)

2. *How can we reduce the production of Fake News? (Select all that apply)*

   a) Increase in Media and Information Literacy (Correct)

   b) Checking the facts (Correct)

   c) Financing and Transparency in Journalism (Correct)

   d) Regulation (Correct)

3. *What should we do when we analyze news?*

   a) Check image source/author (Correct)

   b) Evaluate the veracity of the newspaper (Correct)

   c) Call the author

   d) Confirm if it's an ad (Correct)

   e) Compare Information (Correct)

Lesson 3

–

Disinformation and misinformation

In this lesson an attempt has been made to clarify the difference between two terms – disinformation and misleading information (misinformation). They are often incorrectly used interchangeably. The difference between the two is the intention of the sender of the message. Misinformation is a message that is incorrect, misleading, partially untrue or completely false. It is communicated without a direct intent to deceive. Disinformation is false information that is published with the intention of misleading people. The person who disseminates such a message knows perfectly well that it is false and wants to deceive the recipients.

However, both misinformation and disinformation are dangerous phenomena, both of which provide people with false information and are used to deceive and manipulate.

Another concept also linked to the concepts of disinformation and misinformation is information chaos (noise). It is a concept that refers to an excess of information, often not very essential, that makes it difficult to identify what is important and valuable. It is all this superfluous content that pollutes the information message.

In order to consciously use the information gathered on the web, it is essential to select valuable content. Therefore, this lesson is aimed to define what is meant by disinformation and misleading information and what the techniques for deconstructing media content are.

MODULE:	LESSON UNIT:	TOPIC:
Disinformation and Misinformation	2	Disinformation and Misinformation

LEARNING OUTCOMES:

- Identify what is meant by disinformation and misinformation
- Techniques for deconstructing content in the media

STAGES	AIMS	PROCEDURE	RESOURCES
Introduction	• Introduce trainees to the concept of disinformation in the media • Why it is important to be alert to this phenomenon • Misinformation, wrong information	• The trainer introduces the concept of information disorder • The trainer presents the differences between misinformation and misinformation • Trainer presents practical cases of misinformation and misinformation in the media	• Data show and computer • Internet access
CASE STUDY: (duration: 10 mins)	• Presentation of case study • Discussion about the case presented	• The trainer presents a case study • Students view video of Donald Trump's 1st press conference • https://www.theguardian.com/us-news/2017/feb/16/donald-trump-press-conference-administration-defense-media • Students discuss elements that may constitute elements of disinformation	• Data show and computer • Internet access
Desinformation techniques (duration: 15 mins)	• Disinformation deconstruction techniques	• Presentation of techniques for deconstructing disinformation • The deconstruction of images ○ Online tools to identify fake images • The deconstruction of texts	• Data show and computer • Internet access • Computer for students

		○ Validation of texts through other sources	
task **(duration: 25 mins)**	• Content identification	• The trainer proposes an exercise to the students • The trainer hands the materials for the exercise to the students containing different examples of news in digital media • Students in groups or individually choose 1 or more news • Students apply content deconstruction techniques in the media • Students share the results indicating the main conclusions they reached The trainer summarizes the exercise and asks for feedback from the students	• Data show and computer • Internet access • Computer for students
Good Practices (tempo: 10 mins)	• How to be an critical citizen	• Trainer presents strategies for an active and critical citizenship in relation to the content that surrounds us; • Discussion on how we can be critical citizens in relation to the content we consume every day in the media	• Data show and computer • Internet access • Computer for students
FEEDBACK/ Active reflexion (tempo: 5 mins)	• Reflection on the module	• What we learned • How can we apply • how can we improve	

Two interactive quizzes have also been prepared for this lesson, both of which can be used in class and done together with the whole group, or each learner can do them independently at any time.

Quiz 1

The quiz summarises knowledge of three terms – fake news, disinformation and misinformation. The learner's task is to match the concept with its term. The quiz is a test to see if the learners have correctly remembered what the different types of information are. Below the content of the quiz is presented.

Definitions

Misinformation – also information that is spread, regardless of whether there is intent to mislead.

Disinformation – deliberately misleading or biased information; manipulated narrative or facts; propaganda.

Fake news – purposefully crafted, sensational, emotionally charged, misleading or totally fabricated information that mimics the form of mainstream news.

Quiz 2

This is a true-or-false quiz and concerns the phenomenon of deepfake, i.e. creating and publishing false information in the form of videos, audio recordings and photographs. With deepfake, it is possible to obtain realistic but falsified videos that create opportunities for manipulation or deception. An example of this would be the viewer's inability to distinguish between the faces of actors appearing in a film. The quiz aims to raise awareness of the dangers of such a phenomenon. The content of the quiz with the correct answers is given below.

1. Deepfake technology can create almost real but entirely fictional photos and videos from scratch: TRUE
2. Deepfakes use deep learning artificial intelligence to replace the likeness of one person with another in video and other digital media TRUE
3. There are concerns that deep fake technology can be used to create fake news and misleading, counterfeit videos. TRUE

Lesson 4
–
Conscious use of ICT

The lesson summarises and brings together the learners' knowledge and skills for the informed use of information technology. The trainer invites the learners to discuss the role and impact of information and communication technologies on their daily lives. It is important to note here that these technologies do not only cover computer use, but also mobile devices or smartwatches. The discussion can be led in many ways. You can look for pros and cons of using such technology in everyday life; you can focus only on the good points, or you can divide the learners into two groups – one focusing on the good points and the other on the bad points. The exchange of experiences during such a discussion can allow learners to find new and creative uses for digital technology in their daily and professional lives.

In addition to the exchange of experiences, there is a list of good and bad practices in the use of digital technologies to be created during the lesson. The trainer can use the method of brainstorming among the learners and write down all the emerging ideas on the board and then summarise and complete this list. An essential aspect is to collect from the learners their own answers on what they think informed use of information technology is.

One essential use of information technology is to communicate with different groups of people. The trainer can specify the different channels of communication using information technology and the tools used for this purpose and popular in his/her country. It is important to note here that communication with people from different parts of the world was possible all the time by traditional methods, but the use of information technology has greatly accelerated it.

MODULE:	LESSON UNIT:	TOPIC:
Conscious use of ICTs	1	Conscious use of ICTs

LEARNING OUTCOMES:

STAGES	AIMS	PROCEDURE	RESOURCES
Introduction to Information and Communication Technologies: **(duration: 10 mins)**	• Living without information and communication technologies • search for a theme • Find a song (how?) • Communicate with friends (how?)	• What are information and communication technologies • Explore with trainees the role and impact of information and communication technologies in everyday life • Trainer share a video on YouTube https://www.youtube.com/watch?v=7Q67Poh7cGA&ab_channel=DilshanSoftLab	• Data show and internet connection
task **(duration: 10 mins)**	• Find the answer to 1 topic or subject without using search engines	• The trainer provides trainees with a set of questions that require an answer • The trainer provides or indicates available resources to find the answer	• Books or a library
Task: **Conscious use of ICT** **(time: 15 mins)**	• What is the conscious use of information technologies?	• The trainer presents good practices and bad practices in the use of ICT • The trainer collects trainees' opinions on their own ICT usage practices • The trainer and trainees compare what was presented by the trainer in relation to their practices	• Data show and internet connection

Comunicar com recurso às TICS	• Explore the use of different ICTs to communicate to different groups of individuals	• The trainer presents different typologies of ICTs • The trainer presents different formats of content • The trainer gives examples of multidimensional use of ICTs	
task **(tempo: 25 mins)**	• The trainer presents an exercise	• The trainees carry out the exercise presented by the trainer on how to communicate an idea • Trainees should choose the most suitable formats to communicate an idea • The trainees must justify the reasons for their choice • After the exercise, trainees and trainer evaluate the results	• Data show and internet connection
FEEDBACK/ REFLEXÃO ACTIVA (tempo: 5 mins)	• Reflection	• Trainees reflect on what they have learned • Trainees reflect on changes and adjustments to their uses of ICT	

For this lesson, as for the previous ones, there are two multimedia resources available on the 'iAware' platform. These can be used during the lesson, or as independent homework. The purpose of the quizzes is to summarise and test the learners' knowledge.

Quiz 1

'Choose many' quiz. The learner's task is to mark all the correct answers. The quiz focuses on the use of information technology in everyday life.

1.Select some of the ICTs you know:

a) Computer (Correct)

b) Fridge

c) Mobile (Correct)

d) Television (Correct)

e) Internet (Correct)

f) Book

g) Lamp

h) Email (Correct)

i) Pen

2. Would it be possible to communicate with friends on the other side of the world without the use of technology? (Select the most correct option)

a) Yes, easily.

b) Yes, but not so easily.

c) No.

3. How was research done before technological evolution?

a) Using the library.

b) Expert interviews.

c) Attendance to training.

d) Through area magazines.

e) All of the above.

4. What are the possible uses of Technologies?

a) Education

b) Data processing

c) Communication

d) Collection of Information

e) Business

f) All of the above (Correct)

Quiz 2

Similarly to quiz 1, it covers the application of technology to activities of daily living. It highlights that it is already present in almost every aspect of life. The quiz includes questions on the incidence of technology. Its aim is to test the learner's knowledge. The task is to choose one correct answer to the question that appears on the screen. Below the content of the quiz with the correct answers is presented.

1. Is it possible to find music using technology?

a) Yes (Correct)

b) No

2. Can I use technology to cook?

a) Yes (Correct)

b) No

3. Can I communicate with my friends through technology?

a) Yes, if they use the same technologies. (Correct)

b) Yes, under any circumstances.

c) Yes, even without the same technologies.

d) No.

4. Is the use of technology free?

a) Yes

b) Depends on the services used (Correct)

c) No

5. Can the technology be used for educational purposes?

a) Yes (Correct)

b) No

6. What are the most used applications for making presentations?

a) Canva

b) Prezi

c) Slides

d) Keynote

e) PowerPoint

f) None of the previous

g) All of the above (Correct)

7. Which of the options is not considered a social network?

a) Facebook

b) TikTok

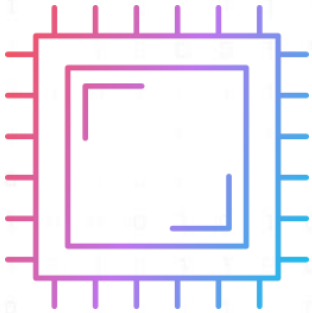
c) Adobe (Correct)

d) Reddit

e) Twitter

f) Whatsapp

g) None of the previous



MODULE 5
-
DIRECTIONS FOR INTERNET DEVELOPMENT, ACTIVE BUILDING OF A GLOBAL COMMUNITY OF E-CITIZENS

The origins of the Internet, the global computer network, can be traced back to the late 1960s in the United States. Since then, it has developed at a very fast pace going through various phases. The Internet is a global computer network and is the largest one in the world, made up of a huge number of smaller networks. It connects computers on all continents, enables the exchange of information and services, and provides access to a vast and growing body of information from all over the world.

The Internet has many meanings for different people. It is a place to meet and exchange ideas, a channel of communication, a collection of information resources available to all, as well as a place to promote and sell goods and services. Like all computer technology, the Internet is developing rapidly. Module 5 brings together the Internet's past and the most interesting directions of its development. The following lesson topics are proposed within this module:

1. ***Past, present and future of the Internet***
2. ***IoT – Internet of Things***
3. ***AI, Big Data and the Cloud***
4. ***E-citizenship***

Lesson 1

–

Past, present and future of the Internet

The aim of this lesson is to understand the context of the emergence of the Internet and the WWW, to understand the difference between the Internet and the WWW. In addition, learners will develop skills to understand the organisation of information on the World Wide Web.

The lesson starts by pointing out the difference between two terms that are often mistakenly used interchangeably – the internet and the WWW (World Wide Web). Although the two terms are related, there are significant differences between them. The internet is a global system of interconnected computer networks and the WWW is a model for sharing information that resides on the internet, i.e. the WWW is only a subset of, and not synonymous with, the Internet.

In the previous modules, learners acquired the skills to use various Internet tools, but this topic also introduces them to concepts such as domain name, hosting protocol and Internet content management systems. They will also learn the differences between WEB 1.0, WEB 2.0 and other ways of using Internet resources.

In addition, there is a practical exercise on how search engines work. Before doing this exercise, trainer can ask learners to share their experiences of using search engines. It is useful here to show learners different methods of narrowing down search criteria.

MODULE:	LESSON UNIT:	TOPIC:
Directions for internet development, active building of a global community of e-citizens	**5.1**	The past, present and future of the internet

LEARNING OUTCOMES:

- Students will understand the context of the emergence of the internet and the WWW
- Students will understand the differences between the internet and the world wide web (WWW)
- Students will become familiar with the different phases of WWW 1.0, 2.0, 3.0 and 4.0.
- Students will be able to identify concepts such as domains, protocols, hosting and servers
- Students will develop skills that enable them to understand how information is organized on the WWW
- Students will be able to identify critical issues associated with internet privacy
- Students will be able to develop safer internet and WWW usage strategies

STAGES	AIMS	PROCEDURE	RESOURCES
Antecedents of the WWW and the historical and social context of the global village. Alan Turing and thinking machines, ARPANET and the need to communicate globally	Understanding the concept of networking, protocols and the differences between the Internet and the WWW	1 - Trainer presents lesson topics 2 - The Trainer explores each trainee's knowledge about the internet and the WWW 3 - Historical context in the emergence of the internet and its actors 4 - Context for the development of the WWW and its actors 5 - Technical characteristics of the Internet and the WWW	• Computer with Internet access.

Case Study **Now and then**	Exercise about the before and after of the web. Imagine 24h without the use of WWW	Reflect on the built-in and ubiquitous logics of using the Internet and the WWW	• Post-its and board pens
The evolution of the WWW	Identification of the different phases of the evolution of the WWW	1 - identification of the main characteristics of the WWW in its different phases 2 - The evolution of the WWW, associated services and life in society	• Computer with Internet access.
Domains, protocols and hosting	Identify the components of a web domain Criar e registar um domínio e um alojamento	1 - What is a domain, subdomain and how to register 2 - Differences between domain and hosting 3 - Content management systems for the web	• PDF reader. • Computer with Internet access.
How data is organized and structured to be available on search engines	What is a Search Engine How information is found and collected and classified	How Search Engines Work - https://www.youtube.com/watch?v=0eKVizvYSUQ&ab_channel=Google Practical exercises based on the following video screening https://www.ted.com/talks/seth_stephens_davidowitz_what_google_searches_can_tell_us_about_who_we_really_are	• Computer with Internet access.
Cookies and Privacy	Understanding Internet and WWW Tracking What is a cookie? How advertising on the WWW works	Understand how tracking works on the WWW Ahat is a cookie Identification of cookie networks Example with lightBeam Preview of web documentary serie - DO NOT TRACK - https://donottrack-doc.com/en/	• Computer with Internet access.

Strategies for safer browsing	Develop skills for safe browsing on the WWW	Development of strategies to identify cookies, their management and preferences defined at the level of different browsers General framework of the GDPR and European legislation on data protection	• Computer with Internet access.

Two multimedia resources have been prepared for the lesson.

Quiz 1

This is a quiz with single and multiple answer questions. Depending on the time in class, the exercise can be done during the lesson or learners can be asked to do the exercise on their own at home. All exercises are posted on the 'iAware' platform and the content of the quiz with correct answers is presented below.

1) Select the correct answer

a) What is the Internet?

b) A type of web browser

c) A global network of computers and electronic devices: X

d) A folder on your computer that stores important files

e) A global collection of different websites

2) Which of the following can you do online? Select all that apply.

a) Pay bills and manage bank accounts X

b) Use search engines to find information X

c) Watch movies and TV shows X

d) Send and receive email and instant messages X

3) Which of the following is NOT a web browser?

a) Windows X

b) Edge

c) Chrome

d) Firefox

4) *When talking about the Web, "link" is an abbreviation for _____.*

   a) *blink*

   b) *hypelink X*

   c) *chain-link*

   d) *superlink*

5) *What are browser tabs mainly used for?*

   a) *Opening multiple web pages in the same browser window X*

   b) *Ensuring that your personal information cannot be seen by hackers*

   c) *Viewing two webpages side-by-side*

   d) *Selecting a Wi-Fi network to connect to*

6) *The WWW and the Internet are the same thing?*

   a) *No, they are different things, but the WWW is part of the INTERNET X*

   b) *Yes, they are the same thing but with different names*

Quiz 2

This is an exercise comprising several parts, the first of which consists of matching WEB 1.0, WEB 2.0 or WEB 3.0 with the correct functionality. The next exercises are questions where learners mark the correct answers. The quiz can be done with the learners in class as a lesson summary or they can be asked to do it themselves at home. The content of the quiz with the correct answers is given below.

1) Match the following words in the correct baskets

Basket 1 – Web 1.0

Basket 2 – Web 2.0

Basket 3 – Web 3.0

a) It's made up of static pages connected to a system via hyperlinks

b) Participative social Web

c) Wikis and blogs

d) It contains dynamic content that responds to the user's input

e) Read-write-interact

f) Waves and live streams

2) Choose the correct answers

a) A cookie is a software that you can download and install

b) A cookie is a text file that contains basic information about your location, operative system, and language that is placed on your browser by the web site that you are visiting

c) A cookie is an application used by the advertising networks

d) A cookie is a sweet

3) *True or false?*

I'm must accept cookies to navigate a website: FALSE

4) *Choose the correct answer*

a) *A first-party cookie is a cookie set in your browser by the web site you are visiting X*

b) *A first-party cookie is a cookie set in your browser by a different web site than the one you are visiting*

5) *Choose the correct answer*

c) *A third-party cookie is a cookie set in your browser by the site you are visiting*

d) *A third-party cookie is a cookie set in your browser by a different web site than the one you are visiting X*

6) *Choose the correct answers*

a) *Navigating in private mode, the browser won't save:*

b) *Your browsing history*

c) *Information entered in forms*

d) *Cookies and site data*

e) *All the answers are correct X*

Lesson 2

-

IoT – Internet of Thing

In its simplest terms, the Internet of Things (IoT) is the concept of devices that can connect to the internet or to other devices, either directly using wireless networks or, rarely, via cables. 'Things' are understood as everyday devices such as modern phones, cameras, fitness watches, home automation and medical instruments, agricultural machines, supply chains, industrial robots and even traffic signals. In other words, the Internet of Things is a network of interconnected devices that can communicate with each other and share data with users over the internet. IoT devices can connect via the internet and are often equipped with various sensors to enable them to collect data. An IoT device can be useful on its own, but when used with multiple devices at the same time, it has even more value. One of the objectives of this lesson is to understand the concept of the Internet of Things and acquire the skills to identify IoT devices, tools and systems. The trainer may ask the learners for examples of IoT devices they have in their homes and use every day.

Given that more and more devices are smart and connect to the internet, the size and importance of the internet of things is growing. If the trainer has previously created a list of IoT items with the learners then the learners will certainly notice that it is very extensive. Various devices ranging from machines in a factory, electrical substations to buildings and infrastructure can all be part of the IoT, and the number of connected devices is increasing every day. Manufacturers, utilities, place authorities, numerous organisations and ordinary people all the Internet of Things.

IoT technology enables the automatic collection of data from various functions. Unfortunately, devices with weaker security features are easily targeted by online criminals. Invasion of privacy, theft of data collected by devices (e.g. photos, audio recordings) are just a selection of the risks that can be encountered. Therefore, another aim of this lesson will be to acquire an awareness of the risks associated with the Internet of Things and to know what precautions to take when using this technology.

MODULE:	LESSON UNIT:	TOPIC:
Directions for internet development, active building of a global community of e-citizens	2	IoT - Internet of Things

LEARNING OUTCOMES:

- Students will become familiar with the terms IoT and Internet of Things, understanding the concept.
- Students will be able to identify IoT devices, tools and systems.
- Students will be aware of IoT Risks.
- Students will know what precautions to take when using this technology.

STAGES	AIMS	PROCEDURE	RESOURCES
1 - Introduction to IoT - Internet of Things (time: 5 mins) **(Vídeo)**	Explain Internet of Things concept.	The student will watch a video that summarizes the concept of Internet of Things, which will include the following topics: • Explanation of what the IoT consists of and what the main objective of this type of systems and digital tools is; • Approach to device types that can be connected and controlled remotely; • Simple reference to the type of technology that is a essential for creating these interconnected devices; Examples of currently available platforms used to aggregate and interconnect multiple devices.	• Computer with Internet access.

2 - Exercise 1 - Identify IoT devices **(time: 10 mins)** **(Multiple Choice Exercise)**	Realize if the knowledge was acquired by the student.	1. A list of definitions related to the Internet of Things is presented. The student will have to choose the most appropriate option in each case; 2. The teacher names some electronic devices, in order to allow the student to identify which of those presented may be IoT objects. - e.g.: Refrigerator, Television, Air Conditioning, Lock, Sockets, Switches.	• Computer with Internet access.
3 - Summary **(time: 5 mins)** **(PDF File)**	Knowledge Consolidation. Making information accessible in a single document.	After completing Exercise 1, the student will have access to a document that will include a list of simple definitions, which summarize the concept, as well as the different types of devices that may be considered from the IoT.	• Computer with Internet access; • PDF reader.
4 - Case Study - The Risks: Case of Diabetes Devices (Negative) **(time: 15 mins)**	Show how technology can also be used for negative purposes, and can also be potentially dangerous.	Students will see an article with an integration example using the Internet of Things applied to the health area, presenting one of the dangers of this type of device, if they do not have any security approach. Article: https://bit.ly/2JVpZta An example video will also be presented, with different dangers that may exist in the most diverse business areas. Video - Internet of Things Security: https://www.youtube.com/watch?v=pGtnC1jKpMg	• Computer with Internet access.
5 - Exercise 2 - What care should I take? **(time: 10 mins)** **(Multiple Choice Exercise)**	Understand whether the student can identify some of the dangers of the Internet of Things.	The student should be able to recognize the problem mentioned in the case study, as well as identify the precautions to be taken to minimize the risks of using IoT devices. Some questions will be asked, through multiple-choice exercises, related to the mentioned example, to ensure that the student had the correct understanding of the concepts implicit in it.	• Computer with Internet access.

6 - Case Study - Boston Children's Hospital (Positive) **(time: 15 mins)**	Show one of the capabilities of IoT devices.	The student will be confronted with a case study from Boston Children's Hospital, in which it uses Internet of Things devices as a way to improve the transmission of information from different routes to its patients, as a way of reducing the times that they get lost in the hospital or going to a location wrongly. Article: https://bit.ly/38uEtKE	• Computer with Internet access.
7 - Resources - Curiosities and Potentialities of the IoT	Provide content that allows the student to explore the Internet of Things.	In this section, students should find different content related to the IoT, namely: videos, news, websites, or articles. In this section, they will be able to explore IoT Tools and Content, identifying more potential, as well as recognizing more examples of the potential dangers of using devices that use this type of technology (called IoT Devices, or Internet of Things Devices).	• Computer with Internet access.
8 - Final Exercise **(time: 10 mins)** **(Multiple Choice Exercise)**	Assess if the student is familiar with the concept of IoT, can identify the tools, as well as the benefits, dangers, and risks of this technology.	The final exercise follows all the previously presented contents, to validate the acquisition of knowledge through them. In this section, several questions will be asked to the student, involving more general subjects, as well as others related to the benefits and dangers of using IoT technologies.	• Computer with Internet access.

Four multimedia materials are provided for this module, namely one video and three interactive quizzes.

Video – This is a video material introducing learners to the Internet of Things and explaining what it is and intended to be used in the first stage of the class. It can be a starting point for discussions with learners about the various IoT devices they use on a daily basis.

Quiz 1

A quiz in which learners answer questions relating to the concept of the Internet of Things. Their task is to mark the correct answers. It can be used already in the first part of the class as a summary of the introductory task on the topic. The result of the quiz will show whether the learners have understood the Internet of Things concept.

1) *Select the most suitable option. The Internet of Things (IoT) consists of:*

   a) *Make use of technology by applying it to everyday devices, creating through connectivity a network of devices that communicate with each other efficiently, allowing the automation of recurring tasks. (Correct)*

   b) *Transforming devices so that they have access to the internet, facilitating their communication processes.*

   c) *Interconnecting multiple devices over the internet, allowing them to communicate with each other.*

2) *Select the types of components used:*

   a) *Devices*

   b) *Communication Networks*

   c) *Control Systems*

   d) *All Previous (Correct)*

3) *Identify the devices that can be integrated into the IoT:*

   a) *Air conditioning*

   b) *Fridge*

   c) *Sockets*

   d) *switches*

   e) *microwave*

   f) *All Previous (Correct)*

   g) *None of the previous*

4) *Applicability Examples*

   a) *A Vacuum Cleaner can be programmed to clean the house after bedtime.*

   b) *House lamps can emit lights in specific tones during various times of the day, or go out when everyone leaves.*

   c) *The air conditioning can turn on five minutes before you arrive, leaving the room at the correct temperature.*

   d) *Hospitals can use equipment capable of collecting data stored on smartwatches or smart bracelets, optimizing service and facilitating diagnosis.*

   e) *All Previous (Correct)*

Quiz 2

This quiz addresses the dangers of IoT and behaviours associated with safe use of IoT. It involves answering the questions that appear on the screen by ticking the correct answers. The quiz relates to the video presented in class. The content of the exercise is presented below.

1) *In the case of the previous study, which type of devices had a security hole?*
    a) *Insulin Pumps (Correct)*
    b) *Blood Glucose Meters*
    c) *All Previous*

2) *What is the danger of this device being controlled by a hacker?*
    a) *This can be turned off, affecting the user.*
    b) *Improper changes in administered insulin levels. (Right)*
    c) *Changes in administered glucose levels.*

3) *How can companies prevent this kind of attacks?*
    a) *Monitor the Risks*
    b) *Be proactive*
    c) *All Previous (Correct)*

4) *In the video you viewed, which IoT devices were analyzed?*
    a) *lock, doll and router*
    b) *doll, lock and electric jug (kettle) (Correct)*
    c) *smartwatch, doll and electric jug*
    d) *camera in security, microwave and padlock*

5) *What security measures should we take? (Multiple Selection)*
    a) *Regulate the use of technology.*
    b) *Use complex, more secure passwords.*
    c) *Keep systems up to date.*
    d) *Use IoT devices on a separate network.*

Quiz 3

Another quiz related to the use of Internet of Things objects. It contains single and multiple answer questions. Learners mark the correct answers on the computer screen. All the questions included in the quiz are provided below.

1) *What are the benefits of IoT? (Select all applicable options)*

   a) Data Monitoring (Correct)

   b) Real Time Devices

   c) Multi-Tasking (Correct)

   d) Better Time Management (Correct)

   e) Less Control

   f) Cost (Correct)

2) *Can I use a smart plug to power my computer?*

   a) Yes (correct)

   b) No

3) *Select one of the disadvantages of IoT:*

   a) Data Monitoring

   b) Data Breach (Correct)

   c) Less Control

   d) More Employability

4) *Which of the following systems is not a virtual assistant?*

   a) Amazon Homekit (Correct)

   b) Google Assistant

   c) Amazon Alexa

d) Apple HomeKit

e) All Previous

5) Which of the Technologies is not involved in IoT?

a) Connectivity

b) Cloud Computing Platforms

c) High power sensors (Correct)

d) Machine Learning and Advanced Analysis

e) Artificial Intelligence (AI)

6) Can IoT devices be used to improve care in the healthcare sector?

a) Yes (correct)

b) No

7) How can I stay safe when using an IoT device?

a) Keep system up to date.

b) Use a separate network for IoT devices.

c) Avoid unknown brands.

d) All Previous (Correct)

e) None of the previous.

Lesson 3

-

AI, Big Data and the Cloud

The aim of the third lesson is to acquire knowledge about Big Data, artificial intelligence and the concept of the cloud, and to be able to critically evaluate these phenomena, of which every person is a part nowadays. Another aim is to acquire knowledge about the links between people, both individuals and society, and computerised, large-scale intelligent systems.

The ability to collect and process data is becoming an increasingly important factor. Big Data refers to the tendency to search for, retrieve, and collect information from a variety of sources and then analyse and use it for one's own purposes. The most important aspect of Big Data is therefore the processing of information and the practical application of its conclusions, rather than the collection of data itself. Big Data is ubiquitous today. Entities that use it in their operations are, for example, banks, which collect data resulting from movements on user accounts, such as payments made, their volume and the types of goods purchased. Companies releasing their own applications that are downloaded by users on smartphones or tablets are another example. By installing the programme on your device, you most often automatically consent to the application’s access to your own data. Online portals also collecting data through the services they provide constitute yet another example.

The trainer, after giving such a general list of examples of big data sets, the trainer may allow the learners to come up with some examples of their own. Ideally, these should be collections they deal with on a daily basis. After listing a few Big Data sets, the learner can be asked to list the data that is being collected and to think about what benefits the analysis of the collected data can provide for the entity.

Artificial intelligence (AI) is also the topic of this lesson. It can be understood as the ability of machines to exhibit human skills such as reasoning, learning, planning and creativity. Artificial intelligence enables technical systems to perceive their environment, deal with what they perceive and solve problems by working towards a specific goal. The computer receives data that is already prepared or collected with its sensors, processes it and reacts. Future applications of AI are expected to bring huge changes, but artificial intelligence is already present in our daily lives.

In the fifth stage of the lesson, there is another exercise in which the trainer encourages the learners to have a discussion connected with exercise one. The task is to create a note in which the learners write down how they imagine artificial intelligence could implement solutions to social problems, helping humanity as a whole. The trainer can give some hints to encourage learners' discussion:

- *Healthcare – analysis of health data and pattern recognition, which can lead to new medical discoveries and improved diagnostics*
- *Civil protection – by using a wide range of data and pattern recognition, artificial intelligence can provide early warning of natural disasters and enable effective preparation and mitigation of consequences*
- *Preventing disinformation and cyber attacks – AI can detect fake news and disinformation by checking social media information, looking for worrying words and identifying credible data sources. AI systems can help identify and combat cyber attacks and other cyber threats based on continuous data entry, pattern recognition and attack tracking*
- *Environment and wildlife – artificial intelligence helps protect nature and the environment by monitoring populations of endangered species*
- *Infrastructure – artificial intelligence can improve infrastructure obstacles such as energy consumption, water and waste management*

MODULE:	LESSON UNIT:	TOPIC:
Directions for internet development, active building of a global community of e-citizens	3	Artificial Intelligence, Big Data and the Cloud.

LEARNING OUTCOMES:

- Acquisition of **grounded intuitions** about what Artificial Intelligence, Big Data and the Cloud are.
- The **ability to explain** concepts related to client-side, server-side, data, computation and use of computations derived from large datasets.
- The **ability to critically evaluate** AI, Big Data and Cloud systems we are all a part of.
- Acquisition of **grounded intuitions** about the links between people (both individuals and societies) and computerized, large-scale, intelligent systems.

STAGES	AIMS	PROCEDURE	RESOURCES
1 – Artificial Intelligence, Big Data and the Cloud: an introduction (time: 10 mins) **(Video)**	Give students practical intuitions about the notions of AI, Big data and cloud computing that are relatable, rather than too "techy"	Students are be exposed to video contents, which - Introduce current ideas about Artificial Intelligence and about why people are talking so much about it these days. - Explain how and why Big Data exist, with basic notions of client-server architectures using examples such as Google search accounts. - Relate Big Data and the Cloud, using the same example of the Google account. - Explain why the growth of the internet, and the increase in large client-server applications has created a perfect synergy opportunity for AI, Big Data and the Cloud.	• Computer with internet access. • Trainer video

2 - Exercise 1 **Identify and examine AI/Big Data/Cloud Systems we are a part of.** **(time: 20 mins)** **Learning by evaluation**	Identify AI/Big Data/ Cloud systems we are a part of, and have a framework to evaluate what they do, how we relate with what they do, how they are beneficial to us, and what precautions we need to take concerning these systems.	1. We present the student with a list of assessment criteria (in various areas) concerning how data are recorded, stored, processed and actioned upon in ways that affect peoples' lives (e.g., productivity, health, and others). 2. Students are then encouraged to identify at least two applications that use AI, Big Data and Cloud. We provide a general list of examples after allowing the student to come up with some options by themselves. 3. Students evaluate chosen applications using the assessment criteria, writing down their observations and evaluations for each criterion. 4. Students are then encouraged to record a voice memo explaining their evaluation of one of the two applications in a succinct and articulated manner. 5. The teaching team asks students for their consent to use their audio data to support the construction of an AI/ Big Data/ Cloud based system that may in the future help students of this area autonomously.	• Computer with internet access. • A physical or digital note taking device, e.g. a notebook, or notepad. • Provided PDF infographic
3 – Making sense of it: Articulating and relating. **(time: 10 mins)** **Activating new knowledge by articulation and introspection**	Articulation and meaning making on concepts that are probably very new to the audience.	In this exercise, students are encouraged to do some individual introspection based on the evaluation they performed in the previous exercise. The main idea is that they identify how AI/Big Data and the Cloud are already playing a role in their lives, as well as how they could become important in their future. Here we encourage students to become aware of how important it is to understand, at least on a basic level, how these systems work, and how they play a part in the lives of individuals and societies. Students may bring ideas about fairness and ethics into this exercise.	• A physical or digital note taking device, e.g., a notebook, or notepad.

4 Case Study: Facebook **(time: 20 mins)** **Evaluation and analysis of potential dangers: case study**	Understand how AI/Big Data/ Cloud applications have inherent potential dangers, and what we can do about them.	We provide a video that discusses how a combination if AI, Big Data and Cloud was used to experiment with the manipulation of peoples' emotions. Students are encouraged to analyse this content in a structured manner, avoiding speculations. We also provide an evaluation procedure that complements the assessment criteria presented in (2) as a PDF Infographic. Video in English: https://www.youtube.com/watch?v=Tslr8o2CxnQ Vídeo Português: https://www.youtube.com/watch?v=itKgV5K2M8M	• Computer with internet access. • A physical or digital note taking device, e.g. a notebook, or notepad. • YouTube video
5 – Exercise 2. Imagine a world where AI/ Big Data and the Cloud work for Social good **(time 15 min)** **AI/Big Data, the Cloud, the future and Social Good**	Put the intuitions in this context to work by imagining possible application areas that would be helpful to the student and their community	This exercise is based on the notebook created in Exercise 1. Students are expected to create a second section/chapter in which they imagine how AI, Data Driver technologies could implement solutions to social problems, helping humanity as a whole. We provide some hints to get them stated (PDF guide), such as helping communities of elderly people, supporting social inclusion and diversity, or solving the problems concerned online teaching for children	• A physical or digital note taking device, e.g., a notebook, or notepad. • Provided PDF guide.
6 – Reflection and take-home message **(time 5 min)** **Closing activity**	Consolidate in the student's mind the ideas and practises worth remembering after the session	Students are encouraged to look at their notebook as a new learning experience. The goal is to add a new section/chapter with two elements: 1. What is the most important thing I have learnt in this session? 2. What steps can I take to bring this knowledge into actions?	• A physical or digital note taking device, e.g. a notebook, or notepad.

This lesson plan is accompanied by two multimedia quizzes, available on the 'iAware' platform.

Quiz 1

This quiz can be used at the end of the lesson as a summary of what the learners should know after the lesson and can be taken together, e.g. on an interactive whiteboard, or by each learner individually on their computers/tablets. Trainer could also ask learners to take the quiz themselves at home as a self-evaluation task. The quiz consists of ten questions to be answered TRUE or FALSE. The content of the quiz with the correct answers is shown below.

1) *Tech companies like Google and Meta (formerly Facebook) can anticipate our needs with AI trained on Big Data and show ads accordingly. TRUTH*
2) *Cloud Computing offers an array of complicated tech services, so it's only used by companies. FALSE*
3) *AI trained on Big Data can learn more about us than we know about ourselves. TRUTH*
4) *Big Data is related to the collection of web data only. FALSE*
5) *The lower the variety in Big Data (up to a certain threshold) the better it is for AI training. FALSE*
6) *Tech companies can know a lot about us even if we haven't directly interacted with them. TRUTH*
7) *Virtual is the main of the 3 Vs in Big Data. FALSE*
8) *Cloud Computing is a market that offers computing services over radio waves. FALSE*
9) *When tech companies acquire other companies they are mostly after the Big Data they have collected and the future data that can be collected. TRUTH*
10) *Cloud Computing can be used continuously or at irregular and infrequent intervals, which makes it very versatile. TRUTH*

Quiz 2

The quiz contains several questions to be answered by the learners by marking the correct answer on the screen. It can be taken with the learners in individually at home. The quiz content, with an X marking the correct answers, is given below.

1) *The concept Big Data refers to*

   a) Structured data only

   b) Unstructured data only

   c) Structured and unstructured data X

2) *Usually what is considered the primary goal of using Big Data/large data sets?*

   a) Find repeatable business patterns X

   b) Improve software testing

   c) Keep up with regulatory changes

3) *How can AI help farming?*

   a) Real time detection of the land condition, weather predictions by apps

   b) AI cannot help farming and other heavy industries X

   c) Convince more people to join the farming industry

   d) Yielding more crops

Lesson 4
-
E-citizenship

An e-society is otherwise known as an information society. The basic feature of this type of society is the management of information, its rapid flow and processing. The most important commodity in the information society is information and the Internet has become a medium that determines almost every sphere of human activity. It has an impact on spending leisure time, running a business, but also on dealing with official matters. Digital citizens are part of the digital society. They use digital technology to engage with the community and act together with the community.

Digital citizenship can be understood as the connection between users and creators of the digital world and the resulting attitude of consciously and responsibly creating and using new technologies for the benefit of themselves and society. This means that an e-citizen should know what impact new technologies have on people, know the rights and responsibilities and skills to use digital technology tools safely.

The objectives of this lesson are to understand the concept of digital citizenship, to acquire the ability to identify the rights and responsibilities of a digital citizen and to be critical of the changes brought about by digitisation in modern societies. In the first stage of the lesson, learners watch a video on the dimensions of digital citizenship. The aspects presented there are outlined below.

The nine dimensions of digital citizenship depicted in the video comprise:

- Skills in using new technologies
- Access to the internet
- Civil rights and freedoms
- Health
- Communication
- Legal conditions
- Security
- Etiquette

- Trade

The subsequent part of the lesson is based on an analysis of China's Social Trust System. This is a system implemented in China for monitoring and evaluating the behaviour of citizens in terms of compliance with the law and the rules of social intercourse. The system is based on databases that receive information from all kinds of state registers, courts, public administration bodies, but also from city monitoring or mobile applications. The idea behind the creation of the Social Trust System in China is to build a society with a high level of trust, in which individuals and organisations respect the law and non-legal standards of social life. This is done by assigning social ratings to citizens based on their behaviour, which directly translate into facilitations or disadvantages in daily life.

The analysis of this system in class consists of finding information in the information (you can watch the YouTube video recorded in the script) and discussing it. Learners should be able to list the advantages and disadvantages of the Social Credit System and discuss its application in European democratic societies.

MODULE:	LESSON UNIT:	TOPIC:
Directions for internet development, active building of a global community of e-citizens	4	E-citizens, social scores and be a human in modern societies

LEARNING OUTCOMES:

- Students will understand the concept of digital citizenship.
- Students will be able to identify the rights and responsibilities of the digital citizen.
- Students will discuss the Social Credit System, based on the Chinese Social Credit System case study.
- Students will be able to reflect creatively on the changes brought about by digital in contemporary societies.

STAGES	AIMS	PROCEDURE	RESOURCES
1 – Introduction to digital citizenship concept **(time: 15 mins)** **(Video)**	Students will understand the concept of digital citizenship.	The student will watch the explanation about the concept of digital citizenship - What is digital citizenship; - The 9 dimensions of digital citizenship; - Examples of the 9 dimensions of digital citizenship. Video: https://www.youtube.com/watch?v=f4B0q2oOLbs&ab_channel=TeachingsinEducation	Computer with Internet access.
2 - Exercise 1 **Exercise on digital citizenship** **(time: 10 mins)** **(Multiple-choice exercise)**	Understand if the knowledge was acquired by the student, through a multiple choice exercise.	A list of definitions and examples related to digital citizenship is presented. The student will have to choose the most appropriate option in each case.	Computer with Internet access.

3 – Exercise 2 **Rights and Responsibilities of digital citizenship** **(True or False Exercise)** **(time: 10 mins)**	Through in depth exploration of each of the dimensions of digital citizenship, the student must identify citizenship rights and responsibilities.	A list of situations is presented, and students will have to identify which of the situations are rights or responsibilities of the digital citizen.	Computer with Internet access.
4 - Summary **(time: 5 mins)** **(PDF File)**	Consolidate knowledge and gather information in a single document, in an accessible way.	After completing the exercise, the student will have access to a document that will include a list of definitions on the dimensions of digital citizenship, and a list of rights and responsibilities regarding digital citizenship.	PDF reader.
5 – Case study – the Chinese social credit system **(time: 8 mins)** **(news story)**	To display knowledge about a citizenship configuration based on the quantification of citizenship actions, through algorithms and platforms.	Será apresentada uma notícia/reportagem sobre o Sistema de crédito social chinês. Students will read/watch a news story on the Chinese Social Credit System. News story: https://www.youtube.com/watch?v=0cGB8dCDf3c&ab_channel=NBCNews	Computer with Internet access.
6 - Debate on social credit systems (time: 10 mins) **(Reflection and debate)**	Discuss the implementation (advantages and disadvantages) of the Social Credit System in European democratic societies.	Students should list the advantages and disadvantages of the Social Credit System, and discuss its implementation in European democratic societies.	Computer with Internet access.

7 - Manifesto for digital citizenship **(time: 3 mins)** **(Video)**	To get familiar with forms of civic participation.	The student will read/watch an excerpt from the Manifesto for digital citizenship. Video (full-lenght): https://www.youtube.com/watch?v=-aWRpwjj5VE&ab_channel=CentrodePesquisaAtopos	Computer with Internet access.
8 – Exercise 3 **Creative Writing**	Imagine, in a creative way, how human beings' everyday life will be, in societies of the future	The student must use the imagination, as well as the knowledge acquired throughout the course, to write a short narrative (up to 350 words) or poem (up to one page) about how the human being's day-to-day (or an aspect of everyday life) will be in the year 3000, imagining the interaction between human and technology (IoT, AI, clouds…).	Computer with Microsoft Word or other word processor software.
9 - Resources – To be human in modern societies	Provide content that allows the student to explore contemporary social thinking about the human being in modern societies.	Nesta secção os estudantes deverão encontrar diversos conteúdos relacionados com o tema, de diferentes tipos, nomeadamente: vídeos, notícias, websites ou artigos. Students will find different content related to the theme, of different types, namely: videos, news, websites and articles.	Computer with Internet access.
10 – Final Exercise	Assess whether the student is familiar with the concept of digital citizenship, and whether the student can identify the rights and duties of the digital citizen.	The final exercise follows all previously presented content and aims to confirm the acquisition of knowledge. Several questions will be asked to the student, involving matters related to digital citizenship, and the rights and responsibilities of the digital citizen.	Computer with Internet access.

Two multimedia quizzes are provided for this lesson plan.

Quiz 1

The quiz may be taken with the learners during the lesson or they may be asked to take it on their own at home. The quiz consists of true or false sentences. The learner's task is to read the sentence, analyse it and mark the correct answer – true or false?

Answer True or False

- Digital citizenship refers to the responsible use of technology by anyone who uses computers, the Internet and digital devices to engage with society at any level. (True)

Answer True or False

- Negative digital citizenship involves cyberbullying, irresponsible use of social media, and a general lack of knowledge about how to use the Internet safely (True)

Quiz 2

The quiz consists of two types of questions – a single-answer test and a true/false task. The learner marks the correct answers on the computer screen or mobile device. The content of the quiz along with the correct answers is shown below.

Indicate the correct answer

1. *Digital Footprint refers to our credentials for accessing social networks*
2. *Our citizen card*
3. *The personal information we leave when using the internet (x)*
4. *None of the answers are correct*

True or false?

When we use content (an image or text, for example) that we find on the internet for our work, it is not necessary to indicate its origin or author because what is on the internet can be used by everyone (F)

CHAPTER 5

-

TOOLS FOR DIAGNOSING ICT COMPETENCE LEVELS

ICT

Digital competences are a set of core skills for modern humans; they are the combination of knowledge, skills and attitudes that enables people to live, learn and work in a digitally enabled society. Digital literacy influences progress in areas of vital importance to the individual and society as a whole, such as quality of life, the economy, healthcare, education, science, security, agriculture, culture and leisure.

Digital competences have been recognised by the European Parliament as one of the eight key competences necessary for lifelong learning. They are linked to a number of skills that all citizens of the 21st-century Europe should possess in order to ensure their active participation in social and economic life.

Nowadays, digital competence is in high demand. More and more services and activities are moving to the digital sphere and the Internet. Official and medical matters, work as well as learning are all areas that are increasingly easy to master with the right digital skills. The COVID pandemic in particular has proven this to be true. Already now, many daily activities are much more difficult or even impossible without the use of a computer or smartphone. It is therefore worthwhile to develop one's own digital competences and encourage others to do the same.

DIGCOMP

As mentioned in previous paragraphs, the European Parliament and the Council of Europe have identified digital competence as one of the eight most important competences for lifelong learning. Such competences are necessary for active participation in society and constitute the basic skills through which the process of developing specific competences is possible. In this view, digital competence can be defined as the free and critical use of information and communication technologies to achieve goals related to work, employment, learning, leisure and participation in society. Digital competence belongs to transversal skills, i.e. it occurs and is even essential for the acquisition of competences in other areas, for example language skills or cultural awareness. Therefore, an attempt has been made to define what these digital competences actually are and what their scope is. DigComp, a reference framework for the development and understanding of digital competences in Europe (Digital Competence Framework), was prepared and first published in 2013 by the European Commission. The aim was to create a tool to improve citizens' digital competences, and to help plan education and training initiatives in order to improve the level of digital competences.

The European Digital Competence Framework for Citizens, known as DigComp, developed by the European Commission, is a tool for the development of digital competences of citizens. DigComp divides the 21 competences it considers as key into 5 areas. In addition, within these areas there are different levels of proficiency (levels A, B, C). The DigComp framework is designed to facilitate an understanding of what digital competences are and what they are used for in today's world.

The DigComp framework is divided into five areas, including:

1. **Information**
2. **Communication**
3. **Content creation**
4. **Security**
5. **Problem solving**

The Information module is devoted to the collection, organisation and preservation of digital information and the assessment of its importance and purpose. The module discusses tools for efficient and secure retrieval of information resources on the web, how to organise them and how to quickly retrieve the information collected and stored.

The Communication module is a compendium of knowledge on how to communicate with other network users, by means of applications and software, widely available via personal computers and mobile devices, using the latest and free technology in multimedia communication. It facilitates the organisation of professional as well as private work and explains the rules governing these in order to be able to quickly, legally and efficiently achieve one's goals in group and individual work.

The Content Creation module is devoted to the creation and editing of new content (images, audio and video recordings, text documents and presentations), creative combination of information from various sources and in various forms in documents, issues related to intellectual property protection and licences, and to the introduction to programming. In addition to the necessary minimum of theoretical knowledge, the module presents practical use of both commercial and free software as well as tools available on the Internet (file conversion, modification of video recordings, creation of web pages).

The Security module is devoted to how to protect oneself and one's own electronic devices from the dangers to which all Internet users are exposed. In particular, the use of anti-virus software, security features built into the operating

system, managing one's digital identities and the health risks of using modern technologies are discussed.

Module 5 Problem solving is aimed at those interested in self-identifying and solving the most common hardware and software problems and how to safely select and acquire the tools necessary to solve daily problems using ICT. It also covers the use of peripheral devices and how to use multimedia resources and ICT in a creative way to update and deepen one's knowledge of digital competence and how to adapt the acquired solutions to one's needs.

The areas can be divided into two types: areas 1 to 3 focus, by definition, on specific activities and applications inherent in these areas, while areas 4 and 5 can be referred to as any activities that are performed with digital tools.

More information on the DigComp framework (including competence descriptions) is available on the website: https://joint-research-centre.ec.europa.eu/digcomp_en

The 'iAware' programme is no alternative to the training according to the DigComp framework. It is, however, a proposal to develop it and take it to the next level. The content is not duplicated and the 'iAware' programme extends and complements certain competences from the DigComp framework. As can be observed, there is no strictly technical content in the 'iAware' programme; instead, there is a focus on the acquisition of practical skills especially for those with low digital competences.

OVERVIEW OF ICT CERTIFICATIONS

Possession of computer skills has become indispensable in many professional sectors. More and more adults are interested in obtaining a certificate to prove the knowledge and skills they have acquired. We present a selection of certificates that a person with low digital competences can obtain in the different project partners.

ITALY:

EIPASS

The EIPASS certification is undoubtedly one of the most requested computer certifications and recognized by Miur. There are different types of EIPASS certifications, which are distinguished by the audience to which they are addressed: these recognized certificates of computer science can be achieved by both young people and adults, are also useful to obtain training credits and extra points in professional rankings.

EIRSAF

To certify computer skills and demonstrate that you have skills with technological devices and programs in current use you can also point to the Eirsaf certifications, recognized by the Ministry of Education as assessable in the recruitment rankings of teaching staff.

SALVEMINI INSTITUTE

Although it is less known than others, the Salvemini Institute IT certification should not be underestimated, since it is also part of the IT certificates recognized by the Ministry of Education, and therefore valid both professionally and in the public sector.

PORTUGAL:

DIGITAL SKILLS CERTIFICATE

The digital skills certificate recognises and certifies the level of digital and media skills. There are two ways to obtain it: one by attending a training course and the other by testing your own skills. The certificate can be obtained by people aged 18 and over, and priority recipients are those with low digital skills and young people who are neither a part of education nor in employment.

POLAND:

ITPASS

It is a certificate that complies with the DigComp framework in all five knowledge areas. It confirms competence in ICT at three levels. The exam can be taken upon completion of the course or if the learner wishes to independently test their skills.

ECCC

The ECCC certificate is the European Certificate of Digital Competence and covers a variety of areas, among them different levels of proficiency. This allows everyone to flexibly adjust the level and scope of the knowledge being verified. What is more, anyone can take the ECCC examinations (including students at different school levels) and at the same time can choose any module and level of certification of their competences.

Moreover, there are also popular international certifications, an example of which is show below:

ECDL (European Computer Driving License)

It is an international certificate in computer skills which, like a language certificate, certifies competence in the use of computer software. It is aimed at people who want to develop their skills and remain up-to-date with modern technology. There are no age limits in the different types of ECDL certificates. For those with limited digital knowledge, the ECDL e-Citizen certificate has been introduced. ECDL certifications are based on competences subdivided into different areas.

EVALUATION AND SELF-EVALUATION TOOLS

Evaluation is the process of determining whether a project has achieved its objectives and, in the case of training, whether the learners have increased their knowledge and skills. Evaluation of conducted courses is essential as it indicates whether the learners have acquired the expected knowledge, practical skills and increased their competence in a given field.

In order to tailor the content and level to the training group, a survey of the learner's knowledge level can be conducted at the beginning of the training cycle. This can be done in the form of a printed questionnaire or by using a number of online tools. Each learner can also use these tools themselves, which will help them to understand their digital skills, show areas where there is a lack of competence at the appropriate level and facilitate the planning of the training path. The most common tools to be encountered are those based on the competences described in DigComp.

MyDigiSkills

MyDigiSkills, is an evaluation tool in line with the DigComp 2.1 model and based on DigCompSAT. "The European Digital Competence Framework for Citizen", is available in 7 languages and has been translated into Italian by Formez PA within the project "ACCEDI - Ambiente per la Cittadinanza Consapevole con l'Educazione Digitale" promoted by Repubblica Digitale in implementation of the Operational Plan of the National Strategy for Digital Competences.

Those interested, after taking the test on MyDigiSkills, will be able in a few months to deepen the self-assessment on ACCEDI and, on the basis of the areas of strength and weaknesses identified, use the resources available to overcome any gaps in digital competence.

https://mydigiskills.eu/index.php

Europass Test

In this regard, a new self-assessment tool has arrived that is very useful for testing our digital skills. It was proposed by the European Commission with the aim of helping students, but also those who already have a job or are looking for one, to understand their level of competence in relation to the European reference framework. Specifically, it is a test consisting of a series of questions that allow you to receive a detailed assessment report in the different areas of competence examined: Computer Literacy, Communication, Digital Content Creation, Security and Problem Solving.

Based on the assessment obtained, then, the platform will give you the most suitable suggestions: therefore, courses and learning opportunities based on the results obtained, useful to improve your skills.

Digital Skill Voyager

Digital Skill Voyager is a tool developed by the Ministry of Economic Development and the Chambers of Commerce of Italy for the evaluation of digital skills. It is aimed at students and workers and, more generally, at all those who are looking for a specific tool to measure their digital skills and to enhance them on the job market.

Digital Skill Voyager is an online test accessible from the portal www.dskill.eu set up with gamification techniques and although it is an effective and rigorous tool, its execution is fun and dynamic.

Digital Skills Accelerator

It is a self-assessment tool that provides an overview of one's own digital competences according to the DigComp framework. It indicates competences that are strong and those that still need to be improved. When using this tool, it is possible to compare one's results with others and to obtain training recommendations. At the end of the test, the results are given in the form of a 'radar chart'. The tool can be tried out at:

http://www.digitalskillsaccelerator.eu/pl/learning-portal/online-self-assessment-tool/

https://digcomp.digital-competence.eu

This tool will assess the level of each of the 21 competences of the DigComp framework, divided into five thematic areas. The learner solves a short test and then receives a coloured graph indicating the percentage level of each competence.

BIBLIOGRAPHY

1. *Aftański P. (2011), Information society - the new value of the information, Dydaktyka informatyki 6, p.66-73*
2. *Buregwa-Czuma S., Garwol K., Definitions, properties, and functions of information society, Dydaktyka informatyki 6, p.30-37*
3. *Cardoso, G., Costa, A., Conceição, C., and Gomes, M. (2005). A Sociedade em Rede em Portugal. Campo das Letras*
4. *Castells M., Społeczeństo w sieci, Warszawa 2008*
5. *Costa, C., Tyner, K., Rosa, P. J., Sousa, C., & Henriques, S. (2018). Desenvolvimento e Validação da Escala de Literacia Mediática e Informacional para Alunos dos 2º e 3º Ciclos do Ensino Básico em Portugal. Revista Lusófona de Educação, 41, 11-28. http://dx.doi.org/10.24140/issn.1645-7250.rle41.01*
6. *Cruz, J. (2008). Evolução do fosso digital em Portugal 1997-2007: uma abordagem sociológica. Instituto Superior de Ciências do Trabalho e da Empresa.*
7. *Czechowska-Derkacz, B. (2015). Dziennikarstwo obywatelskie – o mediach w rękach odbiorców. W: M. Łosiewicz, A. Ryłko-Kurpiewska (red.), Media, business, culture. T. 1, Social and Political Role of the Media. (s. 545-562). Kinvara Co. Galway: TrueSign; Gdynia: Novae Res.*
8. *Dias-Trindade, S., Moreira, J. A., & Nunes, C. S. (2019). Escala de Auto-Avaliação de Competências Digitais de Professores: Procedimentos de Construção e Validação. Texto Livre: Linguagem e Tecnologia, 12(2). http://dx.doi.org/10.17851/1983-3652.12.2.152-171*
9. *Digital Portugal, https://portugaldigital.gov.pt/en/*

10. *Goban-Klas T., Sienkiewicz P., Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji 1999*

11. *Golka M., (2005) Czym jest społeczeństwo informacyjne?, Ruch prawniczy, ekonomiczny i socjologiczny, rok LXVII, zeszyt 4*

12. *Harzyńska J. (2012), Metody pracy z uczniami dorosłymi, Edukacja Humanistyczna nr 1 (26), 201-206*

13. *Kompetencje przyszłości, red. nauk. Stefan M. Kwiatkowski, Fundacja Rozwoju Systemu Edukacji, Seria Naukowa, t. 3, Warszawa 2018*

14. *Krztoń W., XXI wiek – wiekiem społeczeństwa informacyjnego, Modern Menagement Review, MMR vol. XX, 22 (3/2015)*

15. *Kwiatkowska E., Rozwój intenetu rzeczy - szanse i zagrożenia, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 8(3)*

16. *Lyon, D. (1992). A Sociedade da Informação. Celta Editora.*

17. *Making a European Area of Lifelong Learning a Reality, Komunikat Komisji Europejskiej, COM (2001) 678*

18. *Mikołajczyk K. (2011), Jak uczą się dorośli, czyli co powinien wiedzieć trener o specyfice kształcenia uczestników szkolenia, E-mentor nr 2 (39) / 2011*

19. *Morbitzer J. (2004), z metodyki wykorzystywania komputerów w edukacji, Dydaktyka Informatyki 1, 128-140*

20. *OECD (2019), Getting Skills Right: Future-Ready Adult Learning Systems, OECD Publishing*

21. *Olszewska S. (2013), Learning styles and activating methods in adult education, General and Professional Education, 2/2013 p. 20-25*

22. *Patrício, M. (2014). Aprendizagem Intergeracional com Tecnologias de Informação e Comunicação. Universidade do Minho.*

23. *Pereira, S., Pinto, M., & Moura, P. (2015). Níveis de Literacia Mediática: Estudo Exploratório com jovens do 12º ano. CECS/Universidade do Minho*

24. *Pizzirani, A., Di Gioia, R., Chaudron, S., Draper Gil, G. and Sanchez Martin, J., Privacy safeguards and online anonymity, EUR 28991 EN, European Commission, 2017, ISBN 978-92-79-77231-3, doi:10.2760/30934, JRC109792*

25. *Prywatność w sieci, Raport 2016/2017, IAB Polska*

26. *Punie, Y. and Brecko, B., editor(s), Ferrari, A., DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. , EUR 26035, Publications Office of the European Union, Luxembourg, 2013, ISBN 978-92-79-31465-0, doi:10.2788/52966, JRC83167*

27. *Rabka M., Internet XXI wieku – pułapka zagrożeń dla dzieci, młodzieży i osób starszych w dobie pandemii Covid-19, Współczesne Problemy Zarządzania, vol. 8, 1 (16), 2020, DOI:https://doi.org/10.52934/wpz.85*

28. *Rada Unii Europejskiej (2018), Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kluczowych kompetencji w uczeniu się przez całe życie. Dziennik Urzędowy Unii Europejskiej*

29. *Regulacje ws. sztucznej inteligencji: oczekiwania Parlamentu, Aktualności Parlamentu Europejskiego (21-10-2020) https://www.europarl.europa.eu/news/pl/headlines/priorities/sztuczna-inteligencja-w-ue/20201015STO89417/regulacje-ws-sztucznej-inteligencji-oczekiwania-parlamentu*

30. *Rosa, P., Costa, C., Tyner, K., Sousa, C., & Henriques, S. (2019, July). Development and Validation of the Media and Information Literacy Scale (MILS) for the 2nd and 3rd Cycle of Basic Education in Portugal. Poster session presented at the XVI European Congress of Psychology, Moscow, Russia*

31. *ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu*

takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

32. *Sommer H., Sommer H., Michno J., Oportunities and threats of information society - selected aspects, Kultura – Przemiany – Edukacja, t. III (2015)*

33. *Sztuczna inteligencja: co to jest i jakie ma zastosowania?, Aktualności Parlamentu Europejskiego (04-09-2020), https://www.europarl.europa.eu/news/pl/headlines/priorities/sztuczna-inteligencja-w-ue/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania*

34. *Sztuczna inteligencja: szanse i zagrożenia, Aktualności Parlamentu Europejskiego (24-09-2020), https://www.europarl.europa.eu/news/pl/headlines/priorities/sztuczna-inteligencja-w-ue/20200918STO87404/sztuczna-inteligencja-szanse-i-zagrozenia*

35. *Szumilas-Praszek W., Wojtkowiak M., Internet jako współczesne medium zagrożenia czy edukacji?, Społeczeństwo i Rodzina, nr 37 (4/2013)*

36. *The Adult Education Survey (AES), 2016, Eurostat*

37. *Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48883-5, doi:10.2760/490274, JRC128415*

38. *Wrońska, A., Rywczyńska, A. i Lew-Starowicz, R. (2020). Edukacja – relacja – zabawa. Wieloaspektowość internetu w wymiarze bezpieczeństwa dzieci i młodzieży. Warszawa: Fundacja Rozwoju Systemu Edukacji, Seria Naukowa, t. 6*