# Implementation of the web security and personal data protection in educational systems


BE SAFE ON THE INTERNET

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

# Sumary

# Figures and tables

# 1. HOW MUCH /IF EVER IS WEB SECURITY AND PERSONAL DATA PROTECTION IMPLEMENTED IN THE EDUCATIONAL SYSTEMS (VET/UNI LEVEL..)?

## 1.1. AUSTRIA

There are currently around 200 recognised apprenticeships. The apprenticeship professions cover all sectors of the economy:

- Trade and crafts
- Industry
- Trade
- Bank and insurance
- Transport and Traffic
- Tourism and leisure industry
- Information and Consulting
  (Bundesministerium für Bildung, Wissenschaft und Forschung[1] 2019).

In order to get an accurate picture of the inclusion of data management, data protection, data security, data protection regulations and internet security in the different professions and curricula, the different curricula of the apprenticeships offered in Austria were examined. The results of this study are listed below.

| SPECIAL DIDACTIC PRINCIPLES FOR TEACHING |
| --- |
| In class, current media must be used in consideration of data security and data protection. The documents and calculations necessary for the extra-occupational and professional everyday life are to be made computer-assisted. |

### APPLIED ECONOMICS

**Competence Area: Economic Thinking and Action**

Educational and teaching task:

- The students can compare banking services in both national and international payment transactions, taking into account the conditions, and use them in compliance with data security.

**Competence Area: Organisation and Structure of Archives, Libraries and information sector**

Educational and teaching task:

- Students are able to work with personal and other sensitive data taking into account to deal with the legal framework and to reflect on their handling of data.
- Students will be able to use data back-up and protect data from unauthorized access in their personal and professional environment.

**Competence Area: Media and Information**

Educational and teaching task:

- The students identify and point out potential sources of danger on the Internet,

**Competence Area: Conclusion of contracts and management of documents**

Educational and teaching task:

- The students know potential sources of danger on the Internet and can react to these situations appropriately,
- The students are able to demonstrate careful handling of private and professional information as well as sensitive data and to reflect on their own behaviour,

## APPLIED INFORMATICS

**Competence Area: Information Systems, Man and Society**

Educational and teaching task:

- The students are able to demonstrate careful handling of private and professional information as well as sensitive data and to reflect on their own behaviour,
- The students can use data backup options and protect data from unauthorized access in the personal and professional environment.

**Competence Area: IT Products**

Educational and teaching task:

- The students can use data backup options and protect data from unauthorized access in the personal and professional environment.

**Competence Area: IT Services**

Educational and teaching task:

- The students can Install and configure backup and data protection programs.

## BANK SPECIFIC INTERNSHIP / FINANCE SPECIFIC INTERNSHIP

**Competence Area Economic and Business Management Thinking and Acting**

Educational and teaching task:

- The students handle payment transactions from a business perspective and take data security into account when using electronic banking services

## INFORMATION MANAGEMENT

**Competence Area Management and Organization**

Educational and teaching task:

- The students can use data backup options and protect data in the personal and professional environment from unauthorized access,
- The students are able to demonstrate careful handling of private and professional information as well as sensitive data and to reflect on their own behaviour,

## OFFICE PROCESS

**Competence Area Business Processes**

Educational and teaching task:

- The students process payment transactions from a business perspective and take data security into account when using electronic banking services,

**Competence Area: Workplace Office**

Educational and teaching task:

- The students can use data backup options and protect data in the personal and professional environment from unauthorized access,
- The students are able to demonstrate careful handling of private and professional information as well as sensitive data and to reflect on their own behaviour.

## BUSINESS PROJECT INTERNSHIP

**Competence Area: Economic Thinking and Action**

Educational and teaching task:

- The students Use data protection options and protect data from unauthorized access in the personal and professional environment,

## INFORMATICS AND DATA TECHNOLOGY

**Competence Area: Fundamentals of Reproduction and Printing Technology**

Educational and teaching task:

- The students can use data backup options and protect data in the personal and professional environment from unauthorized access,
- The students can analyse an order and inform the client of possible copyright infringements.

**Competence Area: Project Management and Media Production**

Educational and teaching task:

- The students can apply data protection procedures and describe ways of protecting data while taking current standards into account

## IT SYSTEM CUSTOMER

**Competence area Internet presence of companies**

Educational and teaching task:

- The students can demonstrate data backup and data protection concepts and their possible applications explain,
- The students can name current means of information and communication as well as their use critically reflect.

**Competence Area Web Shop Operation and Support**

Educational and teaching task:

- The students can demonstrate data backup and protection concepts and their possible applications explain.

**Competence Area IT Products**

Educational and teaching task:

- The students can demonstrate data backup concepts and explain their possible uses.

**Competence Area IT Services**

Educational and teaching task:

- The students are able to demonstrate careful handling of private and professional information as well as sensitive data and to reflect on their own behaviour,
- The students can name and explain programs for data backup and data protection.

## DIGITAL INTERNSHIP

**Competence area Internet presence of companies**

Educational and teaching task:

- The students can install and configure backup and data protection programs.

## SPECIAL ELECTRONICS

**Additional specifications for the special module Network Technology: Competence Area: Networked IT Systems**

Educational and teaching task:

- The students can explain aspects of data security and justify the use of appropriate systems.

**Additional Specifications for the Special Module Railway Telecommunications: Competence area Railway Communication Systems**

Educational and teaching task:

- The pupils can explain aspects of data security and justify the use of appropriate systems.

## ELECTRONIC PROJECT LABORATORY

**Additional specifications for the special module Network Technology: Competence Area: Networked IT Systems**

Educational and teaching task:

- The students can set up data protection and security systems.

**Additional Specifications for the Special Module Railway Telecommunications: Competence area Railway Communication Systems Education and Teaching:**

- The students will be able to set up data protection and security systems.

## PHOTO AND MULTIMEDIA TECHNOLOGY

**Competence Area Sales Personality and Service Oriented Behavior**

Educational and teaching task:

- The students are able to demonstrate careful handling of private and professional information as well as sensitive data and to reflect on their own behaviour.

## ADVANCED INTERNSHIP

**Competence Area Salon Management/Cosmetic Institute/Foot Care Institute/Massage Institute**

Educational and teaching task:

- The students can create, manage and evaluate customer files with the help of computers and observe data protection regulations.

**Competence Area Business Processes**

Educational and teaching task:

- The students can process payment transactions from a business perspective, convert foreign currencies and take data security into account when using electronic banking services.

**Competence Area Veterinary Surgery and Administration**

Educational and teaching task:

- The students can use information and communication technologies to communicate with pet owners, taking data protection into account, coordinate and plan appointments, taking into account pet owners' wishes and interests, any disruptive factors and the treatment plan, inform pet owners about treatment procedures, accept questions and complaints and implement case-related solution strategies.
- The students can structure classification systems and assign documents, manage incoming and outgoing mail, and organize the archiving and documentation of treatment documents in compliance with documentation and confidentiality obligations as well as data protection.

## BUSINESS PROJECT INTERNSHIP

**Competence Area: guest care, consulting and sales**

Educational and teaching task:

- The students can handle payment transactions from a business perspective and take data security into account when using electronic banking services.

## HOTEL, RECEPTION AND CATERING INTERNSHIP

**Competence Area: Business Processes**

Educational and teaching task:

- The students can use data backup options and protect data from unauthorized access in the personal and professional environment,
- The students are able to demonstrate careful handling of private and professional information as well as sensitive data and to reflect on their own behaviour.

## DATA TECHNOLOGY AND SYSTEM MANAGEMENT

**Competence Area: Database Development and Data Security**

Educational and teaching task:

- The students know the basics of copyright and data protection and can research copyright and data protection regulations in suitable sources and derive and present consequences for their professional activities.

## DATA PROCESSING

**Competence Area: Database Development and Data Security**

Educational and teaching task:

- The students know user and access rights as well as roles and can explain aspects of data security,
- The students know encryption methods and can explain differences between them.

## IT LAB

**Competence Area: Database Development and Data Security**

Educational and teaching task:

- The students can Implement data backup concepts and configure, test and document backups,
- The students can Apply encryption methods professionally.

## LOGISTICS SYSTEMS

**Competence Area: Business Processes**

Educational and teaching task:

- The students can explain, justify and present guidelines for handling customer data and company data.

## INTERNSHIP IN ORDINATION ADMINISTRATION

Competence Area: Practice Organization and Administration

Educational and teaching task:

- The students can structure classification systems and assign documents, manage incoming and outgoing mail, and organize the archiving and documentation of treatment documents in compliance with documentation and confidentiality obligations as well as data protection,

- The students can Information and Communication Technologies in communication with patients in consideration of data protection,
- The students can Caring for patients at the reception as well as recording and managing data for patient documentation in compliance with data protection and legal regulations.

TECHNOLOGY

**Competence Area: Corona and Bridge Technique**

Educational and teaching task:

- The students can name, explain and apply data protection regulations relevant to their profession, in particular with regard to medical data.

## 1.2. CZECH REPUBLIC

Web security and personal data protection is still not integrated in general educational programs focused on social work. Likewise, there is no institutionalized and systematic support of further education of web security.

Web and internet security and personal data protection are integrated in official educational programs like a small part of the whole subject “Infromatics”. Likewise, there is no institutionalized and systematic support of further education of web and internet security and personal data protection for young adults. In Czech Republic, one may come across a range of activities which are to improve the level of safety not only through education carried out in the formal model (schools, universities) but also non-formal and unsystematic. Commercial companies play a great role in a large-scale, media-promoted actions. The idea of corporate social responsibility (web security is the part of that topic) is especially close to companies operating media field, services of which are used also by young people.

The FEP states the 'Informatics and information and communication technologies' (hereinafter 'Informatics') as one of the compulsory areas in regional education.

Informatics is a wide area, which in the Czech FEP (national curricular documents) covers the area of work with ICT, as well as the area of information literacy and online security, as it is for example in the FEP for general secondary schools:

> *'The realisation, respect and alleviation of negative influences of modern information and communication technologies on society and human health to know the means of prevention and protection from misuse and restriction of personal freedom of the human; gaining data from a higher number of alternative sources and differentiating credible and quality information sources from unreliable and poor-quality ones; realisation of basic*

*legal aspects and ethical principles connected to work with information and computer technology with respect to intellectual property, copyright, personal data and principles of correct citation of authors' works'* (page 63).

Another educational area which covers web security in the scope of formal education is the cross-sectional topic 'Media education', which, according to the FEP for general secondary schools, should help the pupil in the following areas:

- *To develop a critical distance from stimuli coming from media products (so to develop the ability to receive and process media products with the sense of how they are constructed and with which communication intention they are being offered at the market);*
- *To realise the importance of unmediated interpersonal relations (family, partner) and their inner emotional and cognitive dynamics (in many cases contrasting with the stereotypical offer of their portrayal in the media products);*
- *To adopt procedures of rational and controlled treatment of symbolic contents; to support free decision making based on critical evaluation of provided information of unequal character, especially decision-making at the level of the civic dimension of living in society and its separation from the consumer's dimension;*
- *To learn to evaluate the quality and relevance of information sources;*
- *To get the idea about the role of media in the individual types of society and different historical contexts'(page 79)*

Methodological support is provided within the scope of implementation of the Strategy of Digital Education until 2020, as well as within continuous methodological support of teachers during the implementation of the FEP.

Methodological support in the scope of implementing the Strategy of Digital Education includes among other things the pillar 'Support for integration of technologies to schools', which contains the methodological support in the area of digital technologies including also web security and personal data protection, but only like a weak topic. However, these are areas which are still not implemented to a significant degree, as stated in the document 'State of realisation of the Strategy of Digital Education' for the first half-year of 2017. Methodological support within the introduction of the FEP is visible in the area of media education, where the National Institute for Education issued a methodological handbook for teachers.

## 1.3. PORTUGAL

Web security and personal data protection is still not very well integrated in the Portuguese educational system (both for VET and UNI level). However, these two topics are usually covered in

some classes such as “ICT” and “Society and Citizenship”. The last topic is treated at the basic education level in several Portuguese schools and the intent is to create space for the educational development and also promotes responsible, critical and active citizens. In these classes many themes can be covered by the teacher and the web security and online safety are becoming more common.

In ANPRI (Associação Nacional de Professores de Informática) website, we can find numerous resources that can be used by teachers at ICT classes and and by other people. ANPRI is teachers’s association and its activities have real impacts on schools, in particular in ICT curricula. The main aim of ANPRI is to develop an interactive space that enables the technology, pedagogical and didactical diversity of their members.

At this link http://www.anpri.pt/course/view.php?id=164, we can find information, power points presentation and other useful links about the topic “Security, responsibility and respect in digital environment”. ICT teachers are not obligated to use these resources available online, but as they are easily accessed many teachers used them in therir classes.

The main themes covered in this platform are:

- Cyberbullying;
- Passwords;
- Security;
- Responsibility and respect in the digital environment;
- Online responsibility;
- Security in instant messages;
- Internet security;
- Terms and conditions.

Recently, between 14th of January and 4th of March in 2019, DGE - Direção Geral da Educação promoted a MOOC - Massive Open Online Course, related to theme “Cybersecurity in schools”. The goal of this course was to call the attention, both for schools and other stakeholders, for the cybersecurity theme. It was a free course and it offered some basic knowledge for a more secure and informed behavior through mobile devices and virtual supports.

This MOOC was structured in 4 modules and the themes covered were:

- Opportunities and security challenges in the digital world;
- Safe use for networks, informatics systems and digital devices;
- Cybersecurity practices in educational communities;
- Threats and cybercrime/legislation;
- Policies and secure practices in schools.

During this course, the participants have had the opportunity to share some ideas, activities and methodologies related to cybersecurity. This MOOC was specially addressed to the directors of private and public schools and ITC coordinators and administrators, who are more frequently involved in issues related to cybersecurity and security in schools. However, this MOOC was also open for high school and preparatory teachers, psychologists, social workers, etc.

More information about this initiative: www.dge.mec.pt/noticias/tic-na-educacao/abertura-do-mooc-ciberseguranca-nas-escolas.

Figure 1. MOOC "Cibersegurança"


## 1.4. SPAIN

Despite the commitment to the inclusion of ICT in the Spanish educational system, we still find multiple deficiencies in the area of cybersecurity. It is necessary to take measures regarding possible threats that may appear in terms of web security and data protection, to be effective its implementation

Schools offer certain levels of protection, but they do not always offer 100% security. Classroom supervision and control can help, but these cannot be extended to every place where children and young people use the Internet.

In March 2010, the European Commission launched the "Europe 2020 Strategy", which includes the creation of the European Digital Agenda, aiming to make the European Union a technological and digital engine by 2020, while guaranteeing trust and security in the use of Information and Communication Technologies (ICT). Within this European framework, the Council of Ministers on 15 February 2013 approved the creation of the Digital Agenda for Spain with more than 100 lines of action structured around six major objectives, one of which consisted of strengthening confidence in the digital environment.

The Digital Confidence Plan endorses the Digital Agenda for Spain, the European Cybersecurity Strategy and the National Security Strategy. This plan contributes building a trusty environment that improves the development of the digital economy and society, implementing a secure and protected web environment, guaranteeing the safe use of networks and information systems, and responding to international commitments on cybersecurity.

Organic Law 8/2013, “for the improvement of the education quality” shows that ICT will be a value to produce the methodological change that will lead to achieving the quality of education. It also establishes that a responsible use of all these new technologies by students must be present throughout the education system. ICT will also be the main training tool for teachers.

In this sense, only a few administrations have regulated its implementation. Such is the case of Department of Education of the Junta de Castilla y León, which considers it especially important to promote the development of information and communication technologies in education in a safe and responsible way. The Educational Innovation Chief for Teacher’s Training, by Resolution of 17 October 2014, launched a project called "Plan for Security and Digital Trust in Education", as an element of coordination, information, dissemination and promotion of a safer use of the Internet by members in the educational community.

Afterwards this satisfactory experience during the academic year 2014-15, authorities have regulated this project in order to consolidate it and to continue developing it in the coming courses. For this reason, on October 14, 2015 was published the ORDER EDU/834/2015 which regulates the “Plan for Security and Digital Trust in the educational field" in the Community of Castilla y León.

The purpose of this project is to promote a safer, more critical and responsible use of ICTs among all members of the educational community, especially students.

The project aims to achieve the following objectives:

- To promote the digital literacy into the educational community.
- To train on the safe use of the Internet (especially by minors).
- To inform about the most common risk situations faced by minors when surfing the Internet.
- To draw up basic safety plans for each age (children, pre-adolescents, teenagers, etc.).
- To offer a helpline and report unwanted situations, identity usurpations, inappropriate behaviour or inappropriate or illegal content founded.
- To promote and disseminate the good use of ICT in education through any courses, workshops, meetings, conferences, etc.
- Dynamize the safe use of ICT tools in schools.

The Castilla y Leon Ministry of Education conducts 1,420 courses and workshops on digital and trust security with over 38,700 attendees among all members of the educational community, especially in the students of Primary Education (EP) and Compulsory Secondary Education (ESO) of the Community.

Other administrations such as the Junta of Andalucía following the recent appearance of regulations on data protection (Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free circulation of these data) and regulations on ICT security (Decree 1/2011 of 11 January, and Order of 9 June 2016) aim to integrate in this ICT security area a continuous adaptation methodology.

# 2. HOW DO THE MINISTRIES OF EDUCATION REFLECT THE FACT, THAT THE WEB AND INTERNET SECURITY AND PERSONAL DATA PROTECTION IS A HOT TOPIC FOR EVERYONE?

## 2.1. AUSTRIA

The Federal Ministry for European and International Affairs invented the “Austrian Cyber Security Strategy” in the year 2013. “The Austrian Cyber Security Strategy / ACSS (Österreichische Strategie für Cyber Sicherheit / ÖSCS) is a comprehensive and proactive concept for protecting cyber space and the people in virtual space while guaranteeing human rights. It will enhance the security and resilience of Austrian infrastructures and services in cyber space. Most importantly, it will, however, build awareness and confidence in the Austrian society” (Federal Chancellery of the Republic of Austria 2003, p. 4).

The Strategy for Cyber Security is the foundation of national cooperation in this area and is based on the principles of the rule of law, subsidiarity, self-regulation and proportionality. The national and international safeguarding of cyberspace is one of Austria's top priorities. An open and free Internet, the protection of personal data and the integrity of interconnected networks are the basis for global prosperity, security and the promotion of human rights.

> “An integrated cyber security policy must place emphasis on task-sharing between the state, the economy, academia and the civil society. It comprises measures in the following areas: politicalstrategic management, education and training, risk assessment, prevention and preparedness, recognition and response, limitation of effects and restoration as well as the development of governmental and non-governmental capabilities and

capacities. An integrated cyber security policy has to be based on a cooperative approach both at national and international level" (ibid., p. 7).

The Strategy includes seven different fields of action and has defined measures for those (ibid., p. 10-16):

Table 1

| Field of Action | | Measures |
|---|---|---|
| 1 | Structures and processes | • Establishing a Cyber Security Steering Group<br>• Creating a structure for coordination at operational level<br>• Establishing a Cyber Crisis Management<br>• Strengthening existing cyber structures |
| 2 | Governance | • Establishing a modern regulatory framework<br>• Defining minimum standards<br>• Preparing an annual report on cyber security |
| 3 | Cooperation between the government, economy and society | • Establishing a Cyber Security Platform<br>• Strengthening support for SMEs<br>• Preparing a Cyber Security Communication Strategy |
| 4 | Protection of critical infrastructures | • Improving the resilience of critical infrastructures |
| 5 | Awareness raising and training | • Strengthening a cyber security culture<br>• Incorporating cyber security and media competence into all levels of education and training |
| 6 | Research and development | • To strengthen Austria´s research in the area of cyber security |
| 7 | International cooperation | • Effective collaboration on cyber security in Europe and worldwide |

## 2.2. CZECH REPUBLIC

There is a governmental strategy in the Czech Republic called **the Digital Czech Republic v. 2.0**, which offers overall backing to other partial conceptions, and one of which is also the Strategy of Digital Education until 2020, which follows up on the governmental document School for the 21st Century.

One of the priorities of the current **Strategy of Digital Education until 2020** is, among other things, also *'to improve pupils' competencies in the area of working with information and digital technologies'* and *'to develop pupils' thinking of informatics'* (page 15).

Some of the tools of implementation of these priorities are the following measures:

- Modernisation of curricular documents (Framework Educational Programmes – FEP) and namely with regards to the emphasis on the issue of ICT across the curriculum;
- Interconnection of formal and non-formal education and informal learning;
- Support of cooperation of public, private and non-profit sectors by the creation and dissemination of innovations;
- Support of teachers' education in this area;
- Introduction of monitoring in this area.

Thus on a political level, the Czech Republic systematically supports the development of digital competences including the web security and pesronal data protection of pupils and students, especially through the introduction of curricular changes, changes in teachers' education and support of cooperation of public, private and non-profit sectors in this area.

The document is the responsibility of the Ministry of Education, Youth and Sports (MEYS), however, individual measures are often presented as cross-sectorial with other responsible sectors and departments stated explicitly in the given topics.

The area of cyberbullying and other specific online dangers is very explicitly visible within the scope of primary prevention of risky behaviour, which is covered by the **Strategy of primary prevention 2013-2018.**

This strategy sees children and youth as a target group and introduces among other things evaluation standards for awarding certification to an entity, which wishes to be active in this area. Entities, which were up to now certified by the MEYS, focus among other things on the area of cyberbullying.

Cyberbullying is also explicitly mentioned within the scope of methodological documents published by the MEYS on primary prevention; the area of online security as such is still missing.

Within the scope of primary prevention, the MEYS also has a subsidy programme.

MEYS has its own Department of Prevention, which deals with methodological support of regional consulting centres, as well as with certification and subsidy programmes. Furthermore, this structure is supplemented by regional school coordinators of prevention and methodology specialists of prevention within the scope of pedagogical-psychological advice bureaus.

## 2.3. PORTUGAL

At the political level, besides some initiatives carried out in Portugal, there is not much information. However, there are some initiatives/activities related to web and internet security and personal data protection in universities, polytechnic institutes and some private organizations.

The only project that exists in Portugal related to digital competences is "Portugal INCoDe.2030". Portugal INCoDe.2030 is a joint initiative of the governmental areas of Administrative Modernization; Science; Technology and Higher Education; Labor; Planning and Infrastructure and Economy. It is a part of the ICT international context and aims to improve and strengthen Portugal's position in the European Commission's 2017 DESI Index (Digital Economy & Society Index), increasing the country's competitiveness by promoting digital skills.

This project is focused on raising the digital competencies of Portuguese citizens by engaging a broad range of stakeholders because currently only 47% of Portuguese citizens have basic digital skills (the expectation is to raise it to 80% until 2030). INCoDe.2030 operates under five axes (inclusion, education, qualification, specialization and research) and intends to meet three major challenges by 2030:

- Ensure digital literacy and inclusion for the exercise of citizenship. There, this project aims to generalize digital access, use and literacy, in order to fully exercise citizenship and to promote inclusion, where many social interactions happen on the internet and are increasingly mediated by electronic devices;
- Foster specialization in digital technologies and applications, in order to promote occupational qualification and a higher value-added economy;
- Produce new knowledge in international cooperation context.

## 2.4. SPAIN

The MECD together with the Autonomous Communities (CCAA), in a space of collaboration and joint decision, have decided to establish common projects with a statewidel dimension to draw up a Digital Culture Plan for the School.

Within this framework, they have defined a plan for the coming years to develop and implement several projects at the service of its users (teachers, educational managers, students, families).

The reflection process was structured in five groups attending to the five priority projects of the plan:

I. School connectivity.
II. Interoperability and standards.
III. Open multimedia content area.
IV. Paid Educational Resources: Neutral Point.
V. Teaching digital competence.

VI. Spaces of collaboration between Autonomous Communities.

VII. Web and social networks.

Table 2

| Projects | Description |
|---|---|
| I. School connectivity | *To get full access to the Internet for educational centres in coordination with the Autonomous Communities, improving the quality of access in a sustainable way through agreements with the telecommunications sector agents.* |
| II. Interoperability and standards | *To provide educational ICT standards and to promote interoperability standards for the use of ICT within the National Interoperability Scheme framework.* |
| III. Open multimedia content area | *To design the evolution of the Agrega educational repository, to turn it into a common open content space in which the entire educational community can contribute.* |
| IV. Paid Educational Resources: Neutral Poin | *To promote agreements with the different agents involved and to define the structure between digital textbooks suppliers, other educational resources and their potential users.* |
| V. Teaching digital competence | *To establish a new model based on digital competences' development for teachers.* |
| VI. Spaces of collaboration between Autonomous Communities | *To create a collaboration space that could be used as a meeting point between the Autonomous Regions and the Ministry.* |
| VII. Web and social networks | *To create a single educational web and to work out a strategy of active presence within social networks, to foster interaction with the educational community.* |

Notwithstanding the above considerations, the internet evolution has provided to self-regulation contracts a special relevance, leaving the State in a secondary role, because almost of the agreements in this field are regulations combined and committed by the private sector without any governmental component. The formulas that currently have the greatest acceptance are public-private alliances (partnership), which are the intersection of co-regulation and self-regulation agreements.

# 3. TO WHAT EXTENT DO COMPETENCES FOSTERED BY NATIONAL EDUCATIONAL SYSTEMS SUPPORT THE CREATION OF PROFESSIONALS CONNECTED TO WEB AND INTERNET SAFETY AND PERSONAL DATA PROTECTION? WHICH TYPES OF COMPETENCES CONNECTED TO THE WEB SECURITY ARE LEFT BEHIND?

## 3.1. AUSTRIA

The 2018/19 school year brings with it an important change: the introduction of digital basic education as a compulsory elective subject in lower secondary education.

Within four years and for a period of two to four hours per week, the schools acquire competences from a total of eight areas listed in the table below (Saferinternet.at[1] 2019).

Table 3

| Areas of Digital Basic Education | Units | Learning objectives |
|---|---|---|
| 1. Social aspects of media change and digitisation | Digitisation in daily life | • Students can design the use of digital devices in their personal environment.<br>• Students reflect on their own media biography and media experiences in their personal environment.<br>• Students describe possible consequences of increasing digitalisation in their personal daily lives. |
| | Opportunities and limits of digitisation | • Students know important application areas of information technology and information technology professions.<br>• Students are aware of social and ethical issues related to technical innovation.<br>• Students can help shape social development by participating in public discourse. |
| | Health and well-being | • Students reflect on the health problems that excessive use of digital media can cause.<br>• Students avoid health risks and threats to physical and mental well-being related to digital technologies. |
| 2. Information, data and media literacy | Search and Find | • Students formulate their needs for information search.<br>• Students plan their search for information, data and digital content in a targeted and independent manner using suitable strategies and methods (e.g. search terms), appropriate tools and useful sources. |

| | | |
|---|---|---|
| | Compare and Rate | • Students apply criteria to assess the credibility and reliability of sources (source criticism, verifiability of knowledge).<br>• Students recognize and reflect clichéd representations and attributions in media communication.<br>• Students can handle automatically prepared information offers on their own responsibility. |
| | Organize | • Students store information, data and digital content in the appropriate format as a meaningful structure in which they can be found and processed. |
| | Sharing | • Students share information, data and digital content with others through appropriate digital technologies.<br>• Students are aware of the basic principles of copyright and data protection (especially the right to their own pictures) and apply these provisions. |
| 3. Operating systems and standard applications | Basics of the operating system | • Students use the functions of an operating system necessary for normal operation, including file management and the print function. |
| | Word processing | • Students enter texts quickly.<br>• Students structure and format text using images, graphics, and other objects. |
| | Presentation software | • Students create presentations using images, graphics, and other objects.<br>• Students follow basic presentation rules (e.g., meaningful images, short texts). |
| | Spreadsheet calculation | • Students perform simple calculations with a spreadsheet and solve age-appropriate tasks.<br>• Students represent series of numbers in appropriate diagrams. |
| 4. Media design | Reception of digital media | • Students know media design elements and can distinguish between media-specific forms.<br>• Students recognise media as an economic factor (e.g. financing, advertising).<br>• Students perceive the design of digital media and the associated communicative action reflected: the connection between content and design (e.g. manipulation), problematic content (e.g. sexualised, violence glorifying content) as well as stereotypical representations in media. |
| | Producing digital media | • Students experience themselves through creative and diverse use of digital technologies.<br>• Students create digital media using current technologies, possibly involving other media: texts, presentations, audio, video and multimedia learning materials.<br>• Pupils observe the basic rules of media design.<br>• Students publish media products in suitable output formats on digital platforms (e.g. blog) |

| | | |
|---|---|---|
| | Developing content | • Students can update and improve information and content and process it in a way that is appropriate for their target group, media format and application. |
| 5. Digital communication and social media | Interacting and communicating | • Students know various digital communication tools.<br>• Students describe communication needs and corresponding requirements for digital communication tools.<br>• Students assess the effects of their own behavior in virtual worlds and behave accordingly.<br>• Students are aware of problematic messages and use strategies to deal with them (e.g. cyberbullying, hate postings). |
| | Participating in society | • Students understand the Internet as a public space and recognize the benefits and risks associated with it. |
| | Designing digital identities | • Students design and protect their own identities reflected.<br>• Students recognize possibilities of manipulation through digital identities (e.g. grooming).<br>• Students pursue the reputation of their own identities and protect it. |
| | Collaborations | • Students use appropriate tools and technologies in a responsible manner (e.g. Wiki, cloud-based tools, learning platform, ePortfolio). |
| 6. Safety | Protect devices and content | • Students are aware of the risks and threats in digital environments.<br>• Students review the protection of their digital devices and turn to the right people when needed.<br>• Students take precautions to protect their devices and content from viruses and malware. |
| | Protecting personal data and privacy | • Students understand how personally identifiable information can be used and shared.<br>• Students take precautions to protect their personal information.<br>• Students are aware of the risks associated with doing business on the Internet. |
| 7. Technical problem solving | Identify technical needs and opportunities | • Students know the components and functions of a computer and a network.<br>• Students know common proprietary and open application programs and associated file types. |
| | Using digital devices | • Students properly connect the most important components of a computer and identify connection errors.<br>• Students connect digital devices to a network and exchange data between different electronic devices. |
| | Solving technical problems | • Students recognize technical problems in the use of digital devices and report a concrete description of the error to the right places. |

| | | |
|---|---|---|
| 8. Computational Thinking | Working with Algorithms | • Students name and describe processes from everyday life.<br>• Students use, create and reflect codes (e.g. cipher, QR code). |
| | Creative use of programming languages | • Students simply create programs or Web applications with appropriate tools to solve a specific problem or accomplish a specific task. |

## 3.2. CZECH REPUBLIC

E-Safe is a nationwide certified project focused on prevention, education, research, intervention and awareness-raising combined with risky Internet behaviour and related phenomena. In recent years, the project has also focused on the positive use of IT in education and everyday life. The E-Safe project is implemented by the Center for the Prevention of Risky Virtual Communication of the Pedagogical Faculty of Palacký University in cooperation with other organizations.

The E-Safe project specializes in:

a) Cyberbullying and sexting (various forms of extortion, threats, victimization by ICT),

b) Cybergrooming (communication with unknown internet users leading to a personal meeting)

c) Cyberstalking and stalking (dangerous ICT persecution)

d) Risks of social networks (especially Facebook and Instagram)

e) Hoax, spam and fake news

f) Online Addiction (Netolism, Nomophobia)

g) Youtubering phenomenon

h) Misuse of personal data in an electronic media environment.

The basic starting point of the project is working with various target groups, lecture activities, preventive educational events, etc. Lectures/discussions are focused on specific dangerous phenomena and possibilities of prevention and defence against attackers. The idea of the issue is based on model situations and real cases. The events are also multimedia, accompanied by many presentations and video clips.

## 3.3. PORTUGAL

Web and internet safety and personal data protection are included in some schools at “ICT” and “Society and Citizenship” classes.

In the case of "Society and Citizenship", according to the entity DGE the 3 main topics addressed at these classes are Human Rights and citizenship, health and sexual education and other themes related to education. Therefore, the topics related with web security, for instance, still do not have the same level of importance as they are less treated. Besides that, there are some forms of public-private and private partnerships that aims to promote web and internet safety and personal data protection. Some of these activities happen during the whole year (Project "Miúdos seguros na Net"; website "SegurançaNet - Navegar em segurança and program "Comunicar em Segurança) while others happen once a year (for example, Safer Internet Day that happens each year in February).

## 3.4. SPAIN

Online Safety (OS) is included in the curriculum following different paths and levels of intensity. In many education systems, elements of OS are present in the list of skills that must be developed by the ICT subject, but also by a broad range of other subjects that build up personal, social, health and economic competences.

The responsibility of teaching Online Safety topics in the curriculum is shared in the majority of the European countries between the ICT teacher and other teachers. In the countries where OS elements are taught as part of other subjects, teachers (and school heads) are responsible for the methods and content that are taught. Usually they operate and sign agreements with an external expert assist teachers when teaching OS content within the framework of projects or working groups. These agreements provides a wide basis for collaboration in schools and also entails an important preventive aspect through campaigns, studies and materials directly addressed at the main agents in the educational field: pupils, parents and teachers.

In almost all the countries, some form of public-private partnership exists to promote the Online Safety activities. These collaborations can be expressed in sporadic participation of the private actors in conferences and workshops or through the establishment of long-term activities related to infrastructure or methodological projects in schools. In all the cases, during the Safer Internet Day (normally in February each year), private companies collaborate in campaigns to raise awareness and inform parents and children. Usually a wide variety of conferences devoted to topics around children's and young people's safety on the Internet and problems of tackling illegal and harmful content online are presented. In addition, in many European countries, the educational authorities had established some form of public-private partnership concerning the promotion of Online Safety for young people in general and in schools in particular. In some countries, private companies support the public authorities in the purchase of computer equipment or specific software dedicated to protect the Internet connections and to monitor the undesired external access to school computers and networks.

Ministries of Education or other Educational Authorities are normally represented in the national Safer Internet Centres supported by the Safer Internet Programme. In general, the cooperation taking place under the Safer Internet Centres is linked to participation in regular meetings with all the involved partners and exchange of information and expertise. The active participation in the Safer Internet Day of the educational sector is one of the direct effects, but not the only one, since in many countries more intense initiatives are also present.

In Spain, OS is included in a more general curriculum key competence called 'Information process and digital competence'. This skill entails a person being autonomous, efficient, responsible, critical and reflexive when it comes to selecting, dealing with and using information and its sources, as well as different technological tools. It also creates critical and reflexive attitudes concerning information assessment, verifying it when necessary, and respecting the socially agreed behaviour norms to regulate the use of information and its sources. OS has a flexible timetable in the majority of European countries, being taught as a horizontal theme of a wide range of subjects. Generally, schools are responsible for allocating the number of hours devoted to OS and the specific arrangements for content distribution between subjects.

# 4. WHAT TYPES OF LEARNING OPPORTUNITIES ARE THERE OFFERED (COURSES, MASTERS, MOOCS, INTERNSHIPS, ETC.) CONNECTED TO WEB SECURITY? IN WHICH TOPICS ARE THESE LEARNING OPPORTUNITIES FOCUSED?

## 4.1. AUSTRIA

*The following list is only an exemplary one and serves only to illustrate the diversity in this topic and not to provide a detailed current record of the entire Austrian education system.*

Master´s programme: IT-Security (Master of Science in Engineering); University of Applied Science – FH Campus Wien

Subjects during this programme: Applications, Operating Systems, Business Administration, Data Security, Distributed Systems Dependability, IT Security, Information Management, Communicative and Social Skills, Cryptography, Middelware Security, Staff Management, Network Defense, Personality Development, Privacy in Internet, Reliable Network Operation, Statistics, Team Building, VPN Technology, White-Collar Crime, Scientific Working (FH Campus Wien 2019).

Master´s programme: Secure Information Systems (Sichere Informationssysteme); University of Applied Science – FH Oberösterreich

Subjects during this programme: Current Security Issues, Data Protection, Digital Identities, Ethics, Information Management, Communication, Networks, Network Security, Law, Secure Software Engineering, Team Leadership, Scientific Work (FH Oberösterreich 2019).

Course: IT-Security compact (University of Vienna): current threats, passwords, data security, web security, email security, basic endpoint security

Course: Ransomware data encryption made easy (University of Vienna): The term Ransomware, To the past / the present , How do you get infected?, How to encrypt?, How do I protect myself?, What helps? Backups, Ransomware detection, Behaviour Managed devices, Live demos

Course: IT Security: How secure is my data? (University of Vienna):: Why do the hackers care about me of all people? What can I lose? What does hacking actually mean and what do the hackers do with me and my devices? Counterfeiting, deception and fraud (phishing, social engineering, advance payment fraud, ...) Common countermeasures (passwords, virus scanners, encryption, data security ...), their problems and how to deal with them. IT security and cloud services.

Course: Encryption Tools for Daily Use (University of Vienna): Virtual Private Network (VPN); Hard disk encryption and mobile devices; encrypted connections (TLS/SSL - certificate service of the ZID); Mail encryption (PGP/GnuPG, S/MIME); telephony (Skype, SIP, ...); key management, deposit, policy strategies (Universität Wien 2019).

MOOC Course: offered for teachers and educators, in which within 8 online lessons it is explained how to use the Internet in the best possible way in class.

Central topics:

1. How can you make your digital tools safe?
2. Which digital environments of children and young people can also be included in teaching?
3. What about copyright or data protection?
4. How do phenomena such as cyberbullying and hate postings occur?
5. What do you have to be aware of if you want to use digital devices in school? (Saferinternet.at[3] 2019)

## 4.2. CZECH REPUBLIC

Following the Digital Strategy, the DigiCoalition was created. DigiKoalice (Czech National Coalition for Digital Jobs) is an open fellowship of representatives of state institutions, IT

companies, ICT sector, educational institutions, academic assemblies, non-profit organizations, statutory authorities of schools, educational institutions and other entities, that wish to contribute to better digital literacy of citizens of the Czech Republic, to increase their chances of succeeding in the labour market with help of their digital skills and a result, improving the competitiveness of the Czech economy.

Non-formal and informal learning are overall covered by the national Youth Strategy 2014-2020, whose strategic goal number 12 states as one of the priorities: '*To support the development of competence of children and youth for safe and creative usage of the media.*'

Strategic goal number 12 has three main areas, all relevant to media literacy and online safety; they are:

- To support the development of emancipated use of the media, primarily the critical evaluation of media content and understanding the representation of the world in the media;
- To support safe use of the media with regard to the risks which are brought about by the new technologies;
- To motivate children and youth to take a creative approach when creating their own media content.

This area of the Strategy is the responsibility of MEYS and the Ministry of Culture, which work on its implementation in the scope of intersectoral cooperation.

With the exception of occasional projects financed by various sources and very often the ESF or the Erasmus+ Programme, there is no systematic education of youth workers in this area in the Czech Republic.

However, in the field of leisure-based education (according to the Education Act) the youth educators can use the support system of the DVPP for pedagogical workers.

In the field of youth organisations, the Czech Council of Children and Youth, a non-state and independent national youth council, started a project in 2017 supported by the ESF and offering possibilities for further education of employees of youth organizations (no voluntary youth workers allowed according to the national grant scheme). It is up to the youth organisations to decide if media and media safety topics as relevant for their education.

## 4.3. PORTUGAL

In Portugal, the learning opportunities that are offered are:

- **MOOC related to theme "Cybersecurity in schools"** promoted by DGE;
- **Intership/Consortium "Centro Internet mais segura em Portugal"** promoted by iseveral organizations (FCT - Fundação para a Ciência e a Tecnologia; DGE; IPDJ - Instituto Português do Desporto e Juventude, I.P.; APAV - Associação Portuguesa de Apoio à Vítima; Fundação Portugal Telecom; and, Microsoft).

This consortium has two pone lines (linha internet segura and linha aberta) and three websites (SeguraNet - Navegar em segurança; Better internet for kids and Inhope).

1. **Line "Linha internet segura".** APAV is responsible for the management and operationalization. The main purpose of this telephone and online line is to help and respond to doubts and problems related to online security, cyberbullying, bullying and unworthy exposure for young people, adults, teachers and children. The full support is confidential and anonymous.
   More info in the website: www.internetsegura.pt/linha-internet-segura.

2. **Line "Linha aberta".** This telephone line is focused on illegal content (child porn, violence and racism) and criminal prosecution of those who publish this type of content.
   More info in the website: linhaalerta.internetsegura.pt.

## 4.4. SPAIN

They implement different actions to provide learning opportunities:

1. Information actions focus on teachers, students, parents and schools

This type of action is aimed at offering specific information to the different actors of the educational community in relation to the risks that minors may face in the network

In this sense, information actions must be adapted to the training needs of each group, reinforcing the information in each case (there are certain risks that are better known by children that by parents, for example the cyber-bullying).

2. Training actions

Training action should provide concrete guidelines for identifying the risks associated with the use of the Internet and how to deal with them.

In this sense, it is important to offer effective information that allows all groups to feel secure and comfortable when use of new technologies. Therefore, training on existing risks in New

Technologies must be rigorous and practical, and the level should be adapted both children and adults knowledge. Training actions should be configured based on communication.

3. Awareness-raising actions

Awareness-raising actions should be aimed at children, parents, educators, and other members of the educational community. The main objective of the awareness-raising actions is that the entire educational community knows the risks of using New Technologies and implements appropriate measures to ensure web security and an appropriate use of these technologies.

The way in which the Public Administrations are implementing actions designed to further awareness and training in this field is highly varied: preparation of guides and didactic, interactive material, dissemination of good practices, publication of studies, creation of websites, organizing workshops, roundtables, seminars and courses, etc. There are several entities collaborating with these proposals among which stand out INCIBE, IS4K, Local Administrations, Police Department, NGO's and other private entities.

# 5. WHICH EDUCATIONAL CENTRES ARE OFFERING THEM (PUBLIC UNIVERSITIES, VET SCHOOLS, PRIMARY EDUCATION, PRIVATE CENTRES)? IS IT BEING IMPLEMENTED IN THE FORMAL EDUCATION SYSTEM, OR AS PART OF A LIFELONG LEARNING?

## 5.1. AUSTRIA

As described in the previous chapters, it is possible to acquire knowledge about Internet security and data protection through different offers. There are courses from universities of applied sciences, courses at universities and MOOC courses from initiatives. The possibilities in Austria are manifold.

The **master plan for digitisation in education** is fundamental to this. The aim is to gradually incorporate the changes resulting from ongoing digitisation into the Austrian education system across the country.

Work on the master plan began in summer 2018. The plan itself is to be drawn up by the beginning of the 2019 summer semester with the involvement of other ministries and experts. The aim is to implement the plan and the projects and measures contained therein by 2023.

The master plan is divided into three major fields of action (Bundesministerium für Bildung, Wissenschaft und Forschung[2] 2019).

**Field of action 1 "Software" - pedagogy, teaching and learning content**
In the course of a fundamental revision of existing curricula, new teaching and learning content from the field of digitisation is to be systematically incorporated into the curricula. The aim is to reflect a comprehensive basic understanding of how to deal with new content in the curricula and to methodically and didactically take account of digitisation in all subjects in the sense of modern teaching.

**Field of action 2 "Hardware" - Infrastructure, modern IT management, modern school administration**
The infrastructural equipment and the availability of mobile end devices are to be brought to a uniform and comparable standard. The prerequisites should be created for the use of digital instruments and tools in schools throughout the country. School administration is to be simplified by modern applications.

**Field of action 3 "Teachers" - initial, further and continuing education**
Digitisation, new ways of conveying content and ways of appropriating it should be systematically anchored in the training and continuing education of educators.

The Master Plan for Digitisation pursues the following objectives:

- Innovation in methodology and didactics through the pedagogically versed use of digital possibilities in teaching.
- Age-appropriate promotion of digital competences and knowledge as well as critical awareness raising in all types of schools and school levels along clear pedagogical guidelines.
- Increasing interest in technology and technology development, especially among girls.
- Reliable transfer of the digital skills, competences and knowledge required for a successful transition to the labour market.
- Promotion of the creative potential among pupils associated with digitisation and strengthening of talents.

## 5.2. CZECH REPUBLIC

In Czech Republic, this is if fostered by private companies which implement their corporate social responsibility programs including the web security and personal data protection and get involved in alleviating socially unfavorable phenomena. These activities take a form of even

more non-standard forms, from nationwide social campaigns, realized also in old media, through educational actions carried out in local communities, addressed to children and youth, to financing the grant funds for non-governmental organizations involved in shaping media competences among children.

Since 2006 there has also been a non-state organisation called the '**National Centre for Safer Internet**' (Národní centrum bezpečného internetu), also known as 'SaferInternet', undertaking many activities to prevent cyberbullying, help (specifically youth and seniors) victims of cyberbullying and other negative risks posed by the internet and new media. The organisation is cooperating with the Ministry of Education, Youth and Sports and other public authorities and runs several projects in the fields of raising awareness raising and helping. The organisation is also a designated national coordinator of the No Hate Speech Movement in the Council of Europe Youth sector by the Ministry of Education, Youth and Sports. The organisation is supported by several public projects from national, regional as well as EU resources. The main initiatives are Day of Safer Internet, Prague Safe online, and European Month of Cybersecurity, and they provide eSafety Label certification for schools.

## 5.3. PORTUGAL

Currently, several courses are available in Portugal in schools and training institutions. At the next table we can find some courses related to the web security, personal data protection and cybersecurity more particularly in universities, polytechnic institutes, and in a private IT consultant Rumos.

Table 4. Courses related to web security, data protection and cybercrime

| Training | Institution | Modality | Link |
|---|---|---|---|
| Security analyst | Rumos group | Face to face and live training | www.rumos.pt/curso/academia-analista-de-seguranca-presencial-com-live-training/ |
| Cyber security academy | Rumos group | Face to face and live training | www.rumos.pt/curso/academia-cyber-security-presencial-com-live-training/ |
| Cyber security & data protection post graduation | Rumos group | Face to face and live training | www.rumos.pt/curso/pos-graduacao-cyber-security-data-protection-pgcsdp-presencial-com-live-training/ |
| Security studies graduation | Lusófona University | Face to face | www.ulusofona.pt/licenciatura/estudos-de-seguranca |
| Cybersecurity and forensic Informatics master | Polytechnic institute de Leiria | Face to face | www.ipleiria.pt/cursos/course/mestrado-em-ciberseguranca-e-informatica-forense/ |

| | | | |
|---|---|---|---|
| Information security and law in the cyber space | Lisboa University | Face to face | www.universia.pt/estudos/universidade-nova-lisboa/mestrado-direito-seguranca/st/180142 |
| Security politics | Lusíada de Lisboa University | Face to face | old.lis.ulusiada.pt/cursos/anolectivo20132014/1ciclolicenciaturas/politicasseguranca.aspx |
| Cybersecurity post graduation | Europeia University | Face to face | www.europeia.pt/oferta-formativa/formacao-de-executivos/pos-graduacoes/ciberseguranca |
| Personal data protection, privacy and cybersecurity in EU | Autonónoma de Lisboa University | Face to face | www.universia.pt/estudos/universidade-autonoma-lisboa/pos-graduacao-protecao-dados-pessoais-privacidade-ciberseguranca-u/st/235118 |
| Cybersecurity | Bragança polytechnic institute | Face to face | portal3.ipb.pt/index.php/pt/guiaects/cursos/cursos-tecnicos-superiores-profissionais/curso?cod_escola=3043&cod_curso=4087 |
| Cybersecurity and cyberspace | Lisboa University | Face to face | www.universia.pt/estudos/universidade-lisboa/ciberseguranca-ciberespaco/st/262185 |
| Informatics security and ethical hacking | Lusófona de Humanidades e Tecnologias University | Face to face | www.universia.pt/estudos/universidade-lusofona-humanidades-tecnologias/pos-graduacao-seguranca-informatica-ethical-hacking-programa-avancado/st/261282 |
| Information security and cyberspace law master | Naval School | Face to face | escolanaval.marinha.pt/pt/ensino_web/estudosposgraduados_web/Paginas/mestseginfdirciber.aspx |

## 5.4. SPAIN

Web security and data protection is implemented as part of a Lifelong Learning, creating and maintaining a positive attitude to learning both for personal and professional development, where knowledge can be acquired and skill-sets developed anywhere – learning is unavoidable and happens all the time. It should be also convenience to implement this field within the formal education system. In this way we would have a global vision of this topic from a very early age.

Web security plans offered by Universities and other institutions.

Table 5. Universities

| | Program | Centre | Place | Modality | Web |
|---|---|---|---|---|---|
| 1 | Máster en Dirección y Gestión de la Ciberseguridad (para directivos) | AUCAL Business School - Universidad Antonio de Nebrija | Madrid | Online | https://www.aucal.edu/curso/master-en-direccion-y-gestion-de-la-ciberseguridad.html |
| 2 | Máster en Ciberderecho | Campus Internacional de Ciberseguridad - Universidad Católica de Murcia (UCAM) - ECIX Group | Valladolid | Online / Semipresential | https://www.campusciberseguridad.com/master-en-ciberderecho |
| 3 | Máster en Ciberseguridad | Campus Internacional de Ciberseguridad - Universidad Católica de Murcia (UCAM) - Telefónica / ElevenPaths | Valladolid | Online | https://www.campusciberseguridad.com/master-en-ciberseguridad-en-colaboracion-con-telefonica |
| 4 | Título Propio de Máster en Informática Forense y Pericial | Campus Internacional de Inteligencia y Pericia (CIIP) | Madrid | Online | https://www.ciip.es/index.php?option=com_content&view=article&id=202&Itemid=120 |
| 5 | Máster INDRA en Ciberseguridad | Centro Universitario de Tecnología y Arte Digital (U-Tad) | Madrid | Presence-based | https://www.u-tad.com/estudios/master-indra-en-ciberseguridad/ |
| 6 | Máster Internacional en Ciberseguridad y Ciberdefensa | CEU San Pablo | Madrid | Online | https://cisde.es/catalogo-de-cursos/masteres/master-internacional-en-ciberseguridad-y-ciberdefensa |
| 7 | Máster Internacional Universitario en Protección de Datos, Transparencia y Acceso a la Información | CEU San Pablo | Madrid | Semipresential | https://www.postgrado.uspceu.es/pages/proteccion_datos/plan-de-estudios.php |
| 8 | Máster en Seguridad Informática y Hacking Ético Oficial de EC-Council. MSI | CICE Escuela Profesional de Nuevas Tecnologías | Madrid | Presence-based | https://cice.es/curso/master-en-seguridad-informatica-y-hacking-etico-ec-council-msi/ |
| 9 | Máster Internacional en Ciberseguridad y Ciberdefensa. V Edición. | CISDE - Campus Internacional para la Seguridad y la Defensa | Sevilla | Online | https://cisde.es/catalogo-de-cursos/masteres/master-internacional-en-ciberseguridad-y-ciberdefensa |
| 10 | Máster en Ciberseguridad y Hacking Ético | Comunix | Málaga | Online / Presence-based | https://www.comunixgroup.com/producto/master-ciberseguridad-y-hacking-etico/ |
| 11 | Data, Complex Networks & Cybersecurity Sciences | DCNC Sciences | Madrid | Presence-based / Online | https://www.master-dcncsciences.com/ |

| | | | | | |
|---|---|---|---|---|---|
| 12 | Master in Cybersecurity | Escuela de negocios NEXTIBS (Next International Business School) | Madrid | Presence-based | https://escuela-de-negocios.nextibs.com/master-in-cybersecurity/ |
| 13 | Máster de Analista Interncional en Cibercrimen y Ciberdelito | Escuela Internacional de Criminología y Criminalística (EICYC) | Alicante | Online | https://www.eicyc.es/portfolio-items/analista-internacional-en-cibercrimen-y-ciberdelito/ |
| 14 | Master en Ciberseguridad | Euroinnova Business School | Granada | Online | https://www.euroinnova.edu.es/Master-En-Ciberseguridad |
| 15 | Máster Internacional en Tecnologías Avanzadas de la Ciberseguridad | Euroinnova Business School | Granada | Online | https://www.euroinnova.edu.es/Master-Ciberseguridad |
| 16 | Máster certificado Elite® Responsable técnico en ciberseguridad y datos I | Exes | Madrid | Online | https://www.exes.es/master-certificado-elite-responsable-tecnico-en-ciberseguridad-y-datos/ |
| 17 | Máster certificado Elite® Responsable técnico en ciberseguridad y datos II | Exes | Madrid | Online | https://www.exes.es/calendario/master-certificado-elite-responsable-tecnico-en-ciberseguridad-y-datos-ii-distancia-online/ |
| 18 | Master in Cybersecurity | IE School of Human Sciences & Technology | Madrid | Presence-based | https://www.ie.edu/cybersecurity |
| 19 | Máster en Ciberseguridad | IMF Business School - Deloitte | Madrid | Online | https://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica |
| 20 | Máster Presencial en Ciberseguridad | IMF Business School - Deloitte | Madrid | Presence-based | https://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica-presencial |
| 21 | Máster en Ciberseguridad | INESEM Business School | Granada | Online | https://www.inesem.es/Master-En-Ciberseguridad |
| 22 | Máster en Seguridad de la Información y las Comunicaciones | INESEM Business School | Granada | Online | https://www.inesem.es/Master-Seguridad-Informacion-Comunicaciones |
| 23 | Máster en Seguridad Informática | INESEM Business School | Granada | Online | https://www.inesem.es/Master-En-Seguridad-Informatica |
| 24 | Máster en Ciberseguridad | Institut de Formació Contínua-IL3. Universitat de Barcelona | Barcelona | Online | https://il3ciberseguridad.com/ |
| 25 | Máster en Seguridad Informática | Mondragon Unibertsitatea | Guipúzcoa | Online | https://www.mondragon.edu/cursos/es/tematicas/informati |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | ca-telecomunicaciones-sistemas-empotrados/master-en-seguridad-informatica-online |
| 26 | Máster Inter-Universitario en Ciberseguridad | Munics | Pontevedra, A Coruña | Presence-based | https://www.munics.es/ |
| 27 | Máster en Seguridad de la Información Empresarial | OBS Business School | Barcelona | Online | https://www.obs-edu.com/es/master-en-seguridad-de-la-informacion-empresarial |
| 28 | Máster Universitario en Seguridad, Defensa y Geoestrategia | Universidad a Distancia de Madrid (UDIMA) | Madrid | Online | https://www.udima.es/es/master-seguridad-defensa-geoestrategia.html |
| 29 | Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones | Universidad Alfonso X El Sabio (UAX) | Madrid | Presence-based | https://www.uax.es/master-universitario-en-ingenieria-de- seguridad-de-la-informacion- y-las-comunicaciones.html |
| 30 | Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen | Universidad Autónoma de Madrid (UAM) | Madrid | Presence-based | https://www.uam.es/ss/Satellite/es/estudioPropio/Master_en_Analisis_de_Evidencias_Digitales_y_Lucha_contra_el_Cibercrimen.htm |
| 31 | Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC | Universidad Autónoma de Madrid (UAM) | Madrid | Presence-based | https://www.uam.es/Derecho/Master-en-Auditor,-Seguridad,-Gobierno-y-Derecho-de-las-TIC-/ |
| 32 | Máster Universitario en Ciberseguridad | Universidad Carlos III de Madrid (UC3M) | Madrid | Presence-based | https://www.uc3m.es/ss/Satellite/Postgrado/es/Detalle/Estudio_C/1371209197821/1371219633369/Master_Universitario_en_Ciberseguridad |
| 33 | Máster en Ciberseguridad | Universidad Católica de Ávila (UCAV) - Deloitte | Ávila | Online | https://www.ucavila.es/index.php?option=com_content&view=article&id=3511&Itemid=241&lang=es |
| 34 | Máster en Ciberdefensa | Universidad de Alcalá (UAH) Fundación In-Nova | Madrid | Semipresential | https://masterciberdefensa.in-nova.org/ |
| 35 | Máster en Seguridad Informática (Ciberseguridad) | Universidad de Cádiz (UCA) | Cádiz | Presence-based | https://esingenieria.uca.es/docencia/master-en-ciberseguridad-datos-informacion/ https://www.uca.es/wp-content/uploads/2017/07/Seguridad-Informatica-jun17 |

| | | | | | |
|---|---|---|---|---|---|
| 36 | Master en Ciberseguridad y Seguridad de la Información (MCSI) | Universidad de Castilla-La Mancha (UCLM) | Albacete | Presence-based / Online | https://mcsi.uclm.es/ |
| 37 | Máster Propio en Ciberseguridad | Universidad de Granada (UGR) | Granada | Presence-based | https://ucys.ugr.es/master-propio-en-ciberseguridad/ |
| 38 | Máster Universitario en Seguridad Informática | Universidad de Jaén | Jaén | Semipresential | https://www.ujaen.es/estudios/oferta-academica/masteres/master-universitario-en-seguridad-informatica |
| 39 | Máster Universitario en Investigación en Ciberseguridad | Universidad de León (ULE) | León | Presence-based / Online | https://ciberseguridad.unileon.es/masterseguridad.html |
| 40 | Máster Universitario en Ingeniería Informática - Especialización en Ciberseguridad | Universidad de Málaga (Escuela Técnica Superior de Ingeniería Informática) | Málaga | Presence-based | https://www.uma.es/etsi-informatica/info/113641/master-u-ingenieria-informatica-nuevo-plan-2018-2019/ |
| 41 | Máster de Seguridad de la Información y las Comunicaciones | Universidad de Sevilla (US) | Sevilla | Semipresential | https://trajano.us.es/~rafa/seguridad/ |
| 42 | Máster Universitario en Seguridad de Tecnologías de la Información y de las Comunicaciones | Universidad Europea de Madrid (UE) | Madrid | Presence-based | https://madrid.universidadeuropea.es/estudios-universitarios/master-universitario-en-seguridad-de-tecnologias-de-la-informacion-y-de-las-comunicaciones |
| 43 | Máster en Ciberdelincuencia | Universidad Internacional de Cataluña (UIC) | Barcelona | Semipresential | https://www.uic.es/es/estudis-uic/derecho/master-en-ciberdelincuencia/presentacion |
| 44 | Master Universitario en Seguridad Informática | Universidad Internacional de La Rioja (UNIR) | La Rioja | Online | https://www.unir.net/ingenieria/master-seguridad-informatica/549200001557/ |
| 45 | Máster en Seguridad Informática | Universidad Internacional de Valencia (VIU) y Universitat Politècnica de Catalunya (UPC) | Valencia | Online | https://www.universidadviu.com/master-interuniversitario-upc-viu-en-ciberseguridad?var=no&c=I90502M0038&gclid=CNydyfiJgNECFVUo0wodvCkKlQ |
| 46 | Máster en Gestión de la Seguridad Integral | Universidad Internacional Menéndez Pelayo (UIMP) - CSIC - ITEFI | Madrid | Presence-based | https://www.itefi.csic.es/es/content/master-en-gestion-de-seguridad-integral-0 |
| 47 | Máster en Ciberseguridad y Tecnologías Avanzadas | Universidad Isabel I de Castilla (UI1) | Burgos | Online | https://www.ui1.es/oferta-academica/master-en-ciberseguridad |

| | | | | | |
|---|---|---|---|---|---|
| 48 | Máster en Sistemas de Gestión y Seguridad de la Información | Universidad Nacional de Educación a Distancia (UNED) | Madrid | Online | https://www2.uned.es/gestion-seguridad-informacion/ |
| 49 | Ciberseguridad en Sistemas de Control Industrial ICS/SCADA | Universidad Nacional de Educación a Distancia (UNED) | Madrid | Online | https://formacionpermanente.uned.es/tp_actividad/idactividad/9245 |
| 50 | Máster Universitario en Ingeniería de Sistemas y de Control | Universidad Nacional de Educación a Distancia (UNED) | Madrid | Online | https://portal.uned.es/portal/page?_pageid=93,22788364&_dad=portal&_schema=PORTAL&idContenido=1 |
| 51 | Máster en Dirección de Ciberseguridad y Ciberinteligencia | Universidad Pablo de Olavide | Sevilla | Semipresential | https://www.upo.es/postgrado/Master-en-Direccion-Ciberseguridad-y-Ciberinteligencia |
| 52 | Máster Universitario en Ciberseguridad | Universidad Politécnica de Madrid (UPM) | Madrid | Presence-based | https://masterciberseguridad.etsit.upm.es/ |
| 53 | Máster en Seguridad de la Información | Universidad Politécnica de Madrid (UPM) | Madrid | Presence-based | https://www.fi.upm.es/segsi/node/1 |
| 54 | Máster en Gobierno de la Ciberseguridad | Universidad Politécnica de Madrid (UPM) - ISMS Forum Spain | Madrid | Presence-based | https://www.ismsforum.es/curso/27/master-en-gobierno-de-la-ciberseguridad/ |
| 55 | Máster en Ciberseguridad y Privacidad | Universidad Rey Juan Carlos (URJC) | Madrid | Online | https://cybersecuritycluster.es/MCYP/ |
| 56 | Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones | Universitat Oberta de Catalunya - Interuniversitario (UOC,UAB, URV) | Barcelona | Online | https://estudios.uoc.edu/es/masters-universitarios/seguridad-tecnologias-informacion-comunicaciones/presentacion |
| 57 | Máster en Cybersecurity Management | Universitat Politècnica de Catalunya (UPC) | Barcelona | Presence-based | https://www.talent.upc.edu/esp/professionals/presentacio/codi/221100/cybersecurity-management/ |
| 58 | Máster en Redes Corporativas e Integración de Sistemas | Universitat Politècnica de València (UPV) | Valencia | Presence-based | https://www.cfp.upv.es/formacion-permanente/cursos/master-en-inteligencia-de-seguridad--ciberdefensa-y-proteccion-de-infraestructuras-criticas |
| 59 | Máster en Ciberseguridad | Universitat Ramon Llull - La Salle | Barcelona | Presence-based | https://www.salleurl.edu/es/estudios/master-en-ciberseguridad |
| 60 | Máster Universitario en Ingeniería Informática: Seguridad Informática y Sistemas Inteligentes | Universitat Rovira i Virgili | Tarragona | Presence-based | https://www.urv.cat/es/temp/masters-oficials/enginyeria-arquitectura/informatica/master-enginyeria-informatica/ |

| | | | | | |
|---|---|---|---|---|---|
| 61 | Grado en Ingeniería de la Ciberseguridad | Universidad Rey Juan Carlos (URJC) | Madrid | Presence-based | https://www.urjc.es/estudios/grado/3100-ingenieria-de-la-ciberseguridad |

Table 6. Other institutions

| | Centre | Web |
|---|---|---|
| 1 | 1Davinci | https://idavinci.es/ |
| 2 | 3DCUBE Professional Tech Institute | https://www.3dcube.es/ |
| 3 | ACENA Centro de Formación | https://www.acena.net/ |
| 4 | AEI Ciberseguridad | https://www.aeiciberseguridad.es/ |
| 5 | Asociación de Titulados en Ingeniería en Informática (ALI) | https://ali.es/?s=cursos |
| 6 | Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE) | https://www.ancite.es/w3/ |
| 7 | Asociación Nacional de Tasadores y Peritos Informáticos (ANTPJI) | https://antpji.org/ |
| 8 | AUCAL Business School | https://www.aucal.edu/estudios.html |
| 9 | Audea | https://www.audea.com/es/ |
| 10 | Aula Center | https://cursosit.es/ |
| 11 | Avanzo | https://www.avanzo.com/ |
| 12 | Campus Internacional de Ciberseguridad | https://www.campusciberseguridad.com/ |
| 13 | Campus Internacional de Inteligencia y Pericia (CIIP) | https://www.ciip.es/ |
| 14 | Campus Internacional para la Seguridad y la Defensa (CISDE) | https://cisde.es/catalogo-de-cursos |
| 15 | CEINA | https://www.ceina.com/es/ |
| 16 | Centro Criptológico Nacional (CCN-CERT) | https://www.ccn.cni.es/index.php/es/menu-formacion-es |
| 17 | Centro Cultural y Deportivo Tajamar | https://fpprofessionaleducation.tajamar.es/ |
| 18 | Centro de Ciberseguridad Industrial (CCI) | https://www.cci-es.org/formacion |
| 19 | Centro de Formación Empresarial Aura | https://www.auraformacion.es/formacion.html |
| 20 | Centro de Formación en Tecnologías de la Información y Comunicaciones de la Comunidad de Madrid (CFTIC) | https://cftic.centrosdeformacion.empleo.madrid.org/cursos-2016-17 |
| 21 | Centro Universitario de Tecnología y Arte Digital (U-TAD) | https://www.u-tad.com/estudios/area-ingenieria/ |
| 22 | CICE Escuela Profesional de Nuevas Tecnologías | https://cice.es/ |
| 23 | Colegio Oficial de Ingenieros de Telecomunicación (COIT) | https://www.coit.es/servicios/formacion |
| 24 | Computer World University | https://www.computerworlduniversity.es/archive/cursos-expertos-de-computerworld-university |
| 25 | Comunix | https://www.comunixgroup.com/ |
| 26 | Criptored | https://www.criptored.upm.es/formacion/ |

| | | |
|---|---|---|
| 27 | Cyber-C Consultancy | https://www.cyber-c.net/ |
| 28 | Deloitte Cyberacademy | https://cyberacademy.deloitte.es/ |
| 29 | DinoSec | https://www.dinosec.com/es/services.html |
| 30 | Docuformación | https://www.docuformacion.com/cursos-por-temas/ |
| 31 | Escuela de Aprendizaje y Cualificación para el Empleo (EACE) | https://www.eace.es/formacion-especializada.php |
| 32 | Escuela de negocios NEXTIBS | https://escuela-de-negocios.nextibs.com/ |
| 33 | Escuela Internacional de Criminología y Criminalística (EICYC) | https://www.eicyc.es/ |
| 34 | Escuela Superior de Ciberseguridad | https://www.es-ciber.com/cursos/ |
| 35 | Euroinnova Business School | https://www.euroinnova.edu.es/ |
| 36 | Exes | https://www.exes.es |
| 37 | Factor Humano Formación | https://factorhumanoformacion.com/ |
| 38 | Formación TIC Alhambra-Eidos | https://formaciontic.com/Index.aspx |
| 39 | Grupo CFI | https://grupocfi.es/formacion/ |
| 40 | Grupo IOE | https://www.grupoioe.es/ |
| 41 | H4DM | https://h4dm.com/formacion/ |
| 42 | ICEMD - ESIC Business & Marketing School | https://www.icemd.com/ |
| 43 | Icraitas | https://www.icraitas.com/ |
| 44 | IE Law School | https://www.ie.edu/es/law-school/ |
| 45 | IMF Business School - Deloitte | https://www.imf-formacion.com/ |
| 46 | INCIBE | https://www.incibe.es/formacion |
| 47 | Inesdi Digital Business School | https://www.inesdi.com/ |
| 48 | INESEM Business School | https://www.inesem.es/ |
| 49 | Instituto de Ciencias Forenses y la Seguridad | https://www.icfs.es/ |
| 50 | Instituto de Tecnologías Físicas y de la Información (ITEFI) - UIMP - CSIC | https://www.itefi.csic.es/es/ |
| 51 | Internet Security Auditors | https://isecauditors.com/formacion-en-seguridad |
| 52 | ISACA Madrid | https://engage.isaca.org/madridchapter/home |
| 53 | ISACA Valencia | https://engage.isaca.org/valenciachapter/home |
| 54 | Ivantia Cibersecurity | https://ivantia.es/ |
| 55 | Learning | https://learning.es |
| 56 | Logitek | https://www.logitek.es/ |
| 57 | Megafor Security | https://www.megafor.es/ |
| 58 | Mondragon Unibertsitatea | https://www.mondragon.edu/es |
| 59 | MSL Formación | https://www.mslformacion.es/ |
| 60 | NEXTEL - Checkpoint | https://www.nextel.es/category/formacion |

| | | |
|---|---|---|
| 61 | NUNSYS - SERVEF Formación Profesional | https://www.nunsysformacion.com/courses/# |
| 62 | OBS Business School | https://www.obs-edu.com/es |
| 63 | OneseQ | https://www.oneseq.es/ |
| 64 | Pentaquark | https://pentaquark.space/es/inicio/ |
| 65 | Portal formativo | https://www.portalformativo.com/cursos-de-informatica-c_1_47.html |
| 66 | RootedCON | https://www.rootedcon.com/formaciones |
| 67 | S21SEC | https://www.s21sec.com/es/academy/ |
| 68 | SANS Institute | https://www.sans.org/information-security-training/by-location/emea/madrid-es |
| 69 | SEAS | https://www.seas.es/areas/informatica |
| 70 | Securízame | https://cursos.securizame.com/cursos/#cursos |
| 71 | Sidertia | https://www.sidertia.com/Home/Services/Training |
| 72 | SION | https://seguridadinformaticaonline.net/ |
| 73 | Sothis | https://www.sothis.tech/servicio/formacion/ |
| 74 | Stackoverflow | https://www.stackoverflow.es/ |
| 75 | SVT Cloud & Security Services | https://elearning.svtcloud.com/ |
| 76 | TechHeroX | https://techherox.com/ |
| 77 | Technological Institute for Data, Complex Networks & Cybersecurity Sciences (DCNC Sciences) | https://www.master-dcncsciences.com/ |
| 78 | The Security Sentinel | https://thesecuritysentinel.es/ |
| 79 | Universidad a Distancia de Madrid (UDIMA) | https://www.udima.es/es/ |
| 80 | Universidad Alfonso X El Sabio (UAX) | https://www.uax.es/ |
| 81 | Universidad Autónoma de Madrid (UAM) | https://www.uam.es/ss/Satellite/es/home/ |
| 82 | Universidad Cardenal Herrera (CEU) | https://www.uchceu.es/ |
| 83 | Universidad Carlos III de Madrid (UC3M) | https://www.uc3m.es/Inicio |
| 84 | Universidad Católica de Ávila (UCAV) | https://www.ucavila.es/ |
| 85 | Universidad CEU San Pablo | https://www.uspceu.com/ |
| 86 | Universidad de Alcalá (UAH) - Fundación General de la Universidad de Alcalá (FGUA) | https://www.uah.es/es/ |
| 87 | Universidad de Cádiz (UCA) | https://www.uca.es/ |
| 88 | Universidad de Castilla-La Mancha (UCLM) | https://www.uclm.es/ |
| 89 | Universidad de Extremadura (UNEX) | https://www.unex.es/ |
| 90 | Universidad de Granada (UGR) | https://ucys.ugr.es/ |
| 91 | Universidad de Jaén | https://www10.ujaen.es/ |
| 92 | Universidad de León (ULE) | https://www.unileon.es/ |

| | | |
|---|---|---|
| 93 | Universidad de Málaga (UMA) | https://www.uma.es/etsi-informatica/ |
| 94 | Universidad de Oviedo | https://www.uniovi.es/inicio |
| 95 | Universidad de Sevilla (US) | https://trajano.us.es/ |
| 96 | Universidad de Valladolid (UVA) | https://www.inf.uva.es |
| 97 | Universidad de Vigo | https://www.uvigo.gal/ |
| 98 | Universidad Europea de Madrid (UE) | https://madrid.universidadeuropea.es/ |
| 99 | Universidad Internacional de Cataluña (UIC) | https://www.uic.es/es/estudios |
| 100 | Universidad Internacional de La Rioja (UNIR) | https://www.unir.net/ingenieria/ |
| 101 | Universidad Internacional de Valencia (VIU) | https://www.universidadviu.com/ |
| 102 | Universidad Isabel I | https://www.ui1.es/ |
| 103 | Universidad Nacional de Educación a Distancia (UNED) | https://formacionpermanente.uned.es/ |
| 104 | Universidad Pablo de Olavide | https://www.upo.es/portal/impe/web/portada |
| 105 | Universidad Politécnica de Madrid (UPM) | https://www.upm.es/ |
| 106 | Universidad Rey Juan Carlos (URJC) | https://www.urjc.es/ |
| 107 | Universidade da Coruña | https://www.udc.es/ |
| 108 | Universitat Oberta de Catalunya (UOC) | https://estudios.uoc.edu/es/estudia-en-la-uoc |
| 109 | Universitat Politècnica de Catalunya (UPC) | https://www.talent.upc.edu/esp/professionals/searchAV/area/4 |
| 110 | Universitat Politécnica de Valencia (UPV) | https://www.cfp.upv.es/formacion-permanente/index/index.jsp |
| 111 | Universitat Ramon Llull (La Salle) | https://beslasalle.salleurl.edu/es/ |
| 112 | Universitat Rovira i Virgili (URV) | https://www.urv.cat/es/ |
| 113 | Urbiola Formación | https://www.urbiolaformacion.com/ |

# 6. IF THESE EXIST, YOU CAN ALSO INCLUDE SOME EXAMPLES OF SPECIFIC GOOD PRACTICES CARRIED OUT IN YOUR COUNTRIES IN THE EDUCATIONAL FIELD

## 6.1. AUSTRIA

Figure 2. Saferinternet.at[2] 2009

Saferinternet.at
Das Internet sicher nutzen!

The Saferinternet.at is an association supported by the European Union (CEF Telecom/Safer Internet), the Federal Ministry of Education, Science and Research the Federal Chancellery | Department V/5 Youth Policy, as well as two private companies.

Saferinternet.at supports above all children, young people, parents and teachers in the safe, competent and responsible use of digital media. The prepared content is aimed at different target groups: Teachers, parents, young people, youth work and senior citizens.

Contents covered by the initiative:

- Cyberbullying
- Digital Games
- Cell Phone & Tablet
- Social Networks
- Data protection
- Information literacy
- Self-expression
- Problematic contents
- Copyrights
- Viruses, Spam & Co
- Online shopping
- Internet fraud.

The various topics are presented in a variety of ways - there is a news section, FAQs, materials and tips. In addition, there is an event service, brochures on the various topics, a newsletter, counselling services, a youth Internet monitor and the video-based parents' guide "Frag Barbara!" (saferinternet.at[2] 2019).

Since 2005, they have hosted 12,200 workshops and lectures, hosted 1,635 events & activities in Austria, held 14,370 consultations and reached about 152,500 users online per month (Saferinternet.at 2018).

## 6.2. CZECH REPUBLIC

An example of a good practice is a project realized by global Internet services giant – Google. Google in Czech Republic made an assumption that efficient media education may be successfully realized through use of the potential that is in youth. The name of the project contains a term ‘Webrangers’ - namely a person at the age of 13-15, particularly interested in the topic of the Internet, social media and willing to teach other young Internet users how to use the achievements of a global village safely. The project has been carried out in the whole country and one of its partners is the Centre for the prevention of risky virtual communication Faculty of Education of Palacký University in Olomouc. The latter has conducted the research the results of which were presented in the previous parts of this article. The project aims at motivating the

youth from Czech to promote knowledge and experience in the area of safe Internet use. These actions are realized through creating training projects, videos and contests by young people. Candidates who want to meet other people involved in the project have this opportunity during trainings organized in Google Czech Centre in Prague. Educational projects children work on involve all the topics referring to the safe web use, and can take any form. Best projects are rewarded after the end each edition. The list of winning educational projects created by Webrangers are presented on the project website.

## 6.3. PORTUGAL

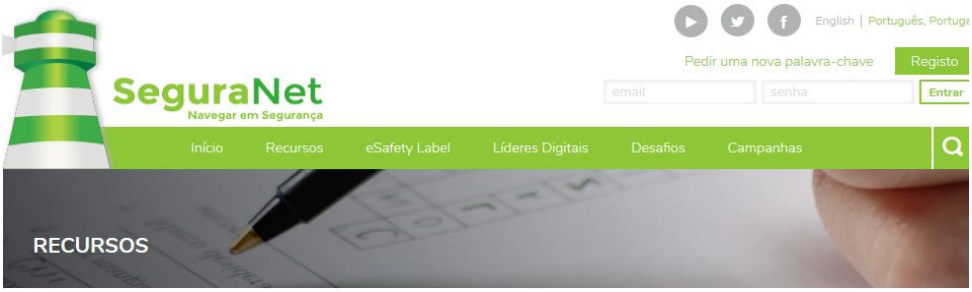
In Portugal there are some initiatives that are or can be carried out in some schools, if they want:

- **"SegurançaNet - Navegar em segurança**": this online website is similar to a data base and includes several information about the web safety oriented to children, schools, young people, fathers and teachers. The main topics covered in this platform are: digital citizenship; online shopping; cyberbullying; and, author rights. Here we can find: animations; games; information; applications; guides; activities; and, billboards. The main formats include presentations, audio, pdfs and videos. The digital security stamp (eSafety label) is an initiative developed by European Schoolnet launched in 2012. This service gives a certification and supports schools and aims to promote a secure environment related to digital technology as an experience of teaching and learning. Last, but not least, in this website we can find the initiative "Líderes digitais 2018-2019" that aims to inspire the students for the promotion of different topics that leads to a more responsible utilization of technology, digital environment.

  The MOOC "Cibersegurança", mencioned before in this report, is included in this initiative.

  More info in the website: [www.seguranet.pt/index.php/pt.](www.seguranet.pt/index.php/pt.)

Figure 3. SeguraNet – Navegar em Segurança




Source: Seguranet.pt

- **Program "Comunicar em Segurança":** this program is promoted at schools and intend to promote a correct use of the internet and ICT. The target groups of this initiative are children, young adults and seniors. This initiative promotes awareness sessions about "how to communicate with safety"; has some online games for the students; has a web series with ten episodes; has also some videos and animations for elementary and preparatory schools. Under this imitative are also organized oadshows in several Portuguese schools.

  More info at: comunicaremseguranca.sapo.pt or at the YouTube channel (https://www.youtube.com/channel/UC-zDTJVhCB93STXOr0DMH8A/videos).

Figure 4. Comunicar em Segurança


Source: Comunicaremsegurança.sapo.pt

- **"Miúdos seguros na NET":** this is a project (runned between 2003 and 2008) that helps families, schools and communities to promote online security for children and young people. The main resources available are articles and a blog.

  More info at www.miudossegurosna.net.

## 6.4. SPAIN

| | |
|---|---|
| CYBERSECURITY MASTER PLAN FOR SCHOOLS<br><br>Link:<br>http://www.ciberexperto.org/ciberexpert/ | The program is implemented to improve children, educational and family environment. It concerns about children experiences on the Internet, showing them how learn about tools, applications and other technological resources that might help them to provide a safer navigation.<br><br>Objectives<br>• To create and carry out activities focused on safety use of the Internet, especially social networks.<br>• To educate children about the risks they may find on the web, and protect themselves from cyber attacks. |

| | |
|---|---|
| | • To provide the necessary tools to improve a safer browsing.<br>• To enable children to acquire competences for safer communication on social networks.<br>• To explain the importance about privacy management. |
| Segureskola Program<br><br>Link: https://gaptain.com/blog/segurescola-centro-escolar-digital/ | Segureskola is a digital accreditation for educational centres that trains in Ethics and Digital Education, in Equality, Awareness of digital risks, it also promotes positive coexistence and guarantees cyber-secure connected environments.<br><br>Objectives<br>• Digital inclusion welfare.<br>• Initially they provide the warnings about internet, social networks and mobile phones risks.<br>• They are able to educate in prevention, identifying the main risks to which your children are exposed. But also they explain the technology benefits and how to improve their career. |
| CIBERALISAL PROJECT<br><br>Link: http://www.ciberalisal.es/ | Ciberalisal is a project born in the IES Alisal from an educational-workshop proposed by the computer science department to promote something different their students. This project awakened the curiosity and interest of a group of students, and the centre decided to go one step further and test talent in an annual competition called 'Cyberolympics', supported by the National Institute of Cybersecurity (INCIBE).<br><br>Objectives<br>• To promote the use of new technologies, especially Internet and social networks.<br>• Talent detection in the field of cybersecurity focus on training, motivation and orientation.<br>• To develop techniques for vulnerabilities detection and mitigation. |
| ENISE AWARDS<br><br>Link: https://www.incibe.es/enise/11enise/premio | This award assesses the best school initiative in the cybersecurity field. Also it has been open to any Primary and Secondary School, Vocational Training and Baccalaureate centres that were able to develop an original initiative to promote cybersecurity among students or in the centre itself. This proposal may have been developed by teachers, students, Parents Associations, or a combination of these groups.<br>The content or subject matter of the initiatives should be inspired in elements that always referring to the nature of the competition: cybersecurity and safe-responsible use of ICT and the Internet, the initiatives may be related to training aspects, preventive action and support. |

# 7. CONCLUSIONS

## 7.1. AUSTRIA

A critical analysis will be developed focusing on the following issues:

- **To what extent have educational systems been adapted to the changing needs of the web security?**
- **Barriers faced by each country in the field of education and web security.**
- **Comparative analysis with partner countries.**
- **You can focus on the topic web security and personal data protection separately, because we suppose that the personal data protection is more implemented in the educational systems than web security.**

In summary, it can be said from the current point of view that there are currently many new developments in the Austrian education system with regard to data security and Internet security. With the introduction of digital basic education, the lower secondary schools are already laying the foundations for an understanding of this topic. Furthermore, the master plan for digitization in education raises hopes that this will be closely integrated into the system in the future. The Austrian Cyber Security Strategy, which will provide a national unit for the implementation of security on the Internet in the future, is fundamental to the whole.

Thus, many different ways have already been identified for dealing with the new challenge of "security on and within the Internet" for all age groups - it is now up to the individual actors to ensure that this also works.

## 7.2. CZECH REPUBLIC

A critical analysis will be developed focusing on the following issues:

- **To what extent have educational systems been adapted to the changing needs of the web security?**
- **Barriers faced by each country in the field of education and web security.**
- **Comparative analysis with partner countries.**

When analyzing the state concerning the web security education in Czech Republic, it is worth to emphasize that it is the country similar in terms of young users' awareness regarding ethreats and that the level of risky behaviors systematically decreases. The key factor differentiating the safety of e-activity of each young network media user is attention of his/her significant others and their readiness to get involved in the process of entering into the cyberspace of digital natives. This state is possible to achieve only through possession of profound knowledge on influence of electronic media by the significant others. The word 'space' should be underlined – space which is a virtual source of cognitive and social experiences for young people, which shapes their sensitivity and their thinking and behavioral patterns in interpersonal relations. In

the technological and educational context, parents and educators face an important task. They are to raise awareness of the youngest generation in the area of critical attitude towards sharing data, which are stored and processed by large international corporations.
During recent years the protection of image on the Internet has become the issue as significant as other, more recognized, e-threats such as: media addiction or cyberbullying. Conscious and efficient alleviation of e-threats in countries, in which social media have become popular in the last few years should include the following principles: diagnosis (also on the international level), actions based on current school curricula and actions of non-governmental organizations, exchange of experiences between institutions involved in media prevention (also on international level) as well as evaluation of the conducted activities.

Education in the field of security and safety is at different level in each country and it is divided into many distinct areas. Teaching of the certain fields of security is strategic due to countries' geographical location, local business or cultural and social aspects. The European Union countries are currently missing some kind of online public database, which would cover the security and safety field and bring together students, researchers and experts interested in the subject.

Schools seem to be the best place to teach children and young adults the digital and critical literacy skills required to maximize opportunities and minimize risks. Schools should focus on education aimed at the safe and responsible use of ICT and should carry major responsibility in teaching them the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies (Becta, 2005; Becta, 2007). The role of the teacher seems to be crucial to ensuring children's e-safety. Teachers are required not only to provide children with knowledge of technical e-safety issues but also to bring them up to be responsible ICT users. Teachers are expected to set good examples for students with respect to such ICT issues as privacy, copyright, data backup, and virus protection (Buettner et al., 2002).

In the matter of e-safety, teachers' behaviour is affected by influences which prevent them from protecting themselves as well as they can (for example pressure on publishing personal information, lax approach or lack of time). These influences originate in their external environment, their personality and lack of expertise and abilities. Lack of expertise prevents teachers from making funded decisions in a specific situation, where their interpretation of a problem can be inexact and they can be put at risk. Take the following citation concerning a teacher's computer getting infected by a virus: "(…) because there was a (window), I wanted to display the content so I clicked on something and it went off. So it must have been (a virus) because instead of displaying some content, it started to do something in my computer". Lack of expertise and ability is demonstrated both by the inexact use of terminology (for example "the cross for clicking is sometimes fake") and by the teachers' explicit remarks: "I don't involve myself in this because I know I am incapable".

Some teachers do not feel good about the imperfection of technical solutions and the possibility that the means of prevention they use could fail.
Teachers are prevented from the safest possible use of ICT by obstacles that originate from the type of person they are, the way they feel and the amount of time they have. Teachers can find themselves in risky situations because they are in a hurry or tired or when they, in their own words, lose concentration. A similar obstacle to security is the amount of remembering that is needed, which leads to rules concerning computer passwords being disregarded. Teachers are aware of disregarding rules and defend their decision by explaining that higher security is not needed due to the type of data they have. If teachers decide to behave in the safest possible way, some security obstacles become security drawbacks. Take the time demands of security, being deprived of certain information (for example on social network sites), forgetting a strong password that has been regularly changed or important messages being marked as spam by an antispam filter. It is necessary to be aware to educate not only user like children, young adults and other, but especially the teachers/trainers to provide their students with appropriate content and form to assure the effectivity and quality of web security education.

Although in EU countries are subtly graded in terms of amounts and types of use and risk, we here group them for ease into four categories or 'ideal types'[1]. Overall, it is striking that high internet use is rarely associated with low risk; and high risk is rarely associated with low use. Rather, the more use, the more risk.

- Lower use, lower risk' countries (Austria, Belgium, France, Germany, Greece, Italy, Hungary) – here children make the lowest use of the internet, and they are below average on all risks apart from meeting online contacts – online and offline; still, it may be expected that as levels of use rise in these countries, so too will risk.
- Lower use, some risk' countries (Ireland, Portugal, Spain, Turkey) have the lowest internet usage, although there is some excessive use of the internet and some problems with user-generated content.
- Higher use, some risk' countries (Cyprus, Finland, the Netherlands, Poland, Slovenia, the UK) make high use of the internet but are high only on some risks, possibly because of effective awareness-raising campaigns, regulatory strategies or strategies of parental mediation of children's internet use.
- Higher use, higher risk' countries (Bulgaria, Czech Republic, Denmark, Estonia, Lithuania, Norway, Romania, Sweden) include both wealthy Nordic countries and Eastern European countries (better called, 'New use, new risk').

[1] Cross national comparison of risks and safety on the internet, Bojana Lobe, Sonia Livingstone, Kjartan Ólafsson and Hana Vodeb, EU Kids online.

Table 7. Country classification based on children's online use and risk (from the EU Kids Online survey)

| | Level of usage | |
|---|---|---|
| **Risk** | **Lower** | **Higher** |
| **Lower** | **Lower use, lower risk**<br>AT, BE, DE, FR, EL, HU, IT<br><br>**Lower use, some risk**<br>ES, IE, PT, TK | |
| **Higher** | | **Higher use, some risk**<br>CY, FI, NL, PL, SI, UK<br><br>**Higher use, higher risk (+ New use, new risk)**<br>BG, CZ, DK, EE, LT, NO, RO, SE |

Wealthier Nordic countries, the UK and the Netherlands have the highest usage across Europe, along with the countries with a lower GDP but more recent introduction of broadband, such as Bulgaria, Romania, Lithuania, Estonia and the Czech Republic.

In Nordic countries and the UK, where 50% of the households had access to the internet for six years or more, daily use of the internet is among the highest. Similarly, daily use is relatively high in countries with newer use of the internet such as Baltic and Eastern European countries. The countries with a longer period (more than 3.5 years) since 50% of households had access to the internet are significantly more likely to experience more online risk – these include Slovenia, the Nordic countries and Estonia. However, Ireland and the UK are countries with older use and a lower degree of risk. Countries with less than approximately three-and-a-half years since 50% of households had access to the internet are significantly less likely to experience online risk. Countries with newer use and high risk include the Czech Republic and Lithuania.

Neither the expected years of schooling nor the percentage of schools that offer and use computers in classrooms has any significant effect on online usage or online risks. However, education has a positive and significant effect on children's digital skills. In countries with 15 years of schooling or more, children are more likely to have above-average digital skills. Similarly, children from countries with a higher percentage of schools that offer and use computers in classrooms (above 45% of schools or more) are significantly more likely to have better digital skills including web security and personal data protection.

## 7.3. PORTUGAL

A critical analysis will be developed focusing on the following issues:

- **To what extent have educational systems been adapted to the changing needs of the web security?**
- **Barriers faced by each country in the field of education and web security.**
- **Comparative analysis with partner countries.**
- **You can focus on the topic web security and personal data protection separately, because we suppose that the personal data protection is more implemented in the educational systems than web security.**

Education is the foundation on which a country is built and educational systems clearly need to be more adapted to the changing needs of the web security in the following years. This situation is also emphasized by the OECD in the report "The future of education and skills - Education 2030" where one of the main challenges is related to cyber security and privacy protection problems.

Even though there are in Portugal some initiatives regarding web security and data personal protection not all schools have access or implement those activities. Besides that, although some schools talk about these themes in some classes (such as Society and Citizenship and ICT) each school doesn't have a plan to to teach and talk about it.

Currently, students are living in a world where horizons for learning are extend well beyond the classroom and with these expanded horizons comes a responsibility for educators to provide environments where students are empowered to achieve academic and personal goals. This new environment requires considerable investment in infrastructure, hardware, software, online resources and professional development.

Therefore, it is crucial to:

- Engage all the community involved in the web security and personal data protection as soon as possible;
- Developing student's digital citizenship through appropriate technology, including online communication etiquette and digital rights and responsibilities;
- Define and review, on frequent basis, the knowledge, skills, attributes and other characteristics that people can and must be trained for, regarding these two topics;
- Stimulate the production of creative and educational online content for all people, that must be simple and accessible for everyone.

The main challenge is to provide to all learners' needs, aligning programmes with the acquisition of 21st century skills because the "one-size-fits-all" approach doesn't work and teachers have an important task to play because they shape the future generations.

The **main barriers** in Portugal in the field of education and web security are:

- Schools don't have a plan and resources to know how to teach and talk about web security and personal data protection;
- The education in Portugal needs more young teachers because, especially in public schools, 80% of the teachers have between 40-59 years;
- The number of computers available for each student is reducing and the acquisition of technological material is made by each school. The acquisition of technological material depends on partnerships available and each school is responsible for buying computers and equipment. In 2016/2017, the number of computers in schools dropped by 31% compared to 2014/2015;
- Digital technologies are constantly changing and teachers need to receive constant training that is not happening. The digital training for each teacher should be based in an innovative environment;
- The Portuguese early drop out of school is higher than in their European counterparts. There are fewer adults between the ages of 30 and 34 to complete higher education which means that they are more likely to have fewer digital competences;
- In Portugal there are a lot of students with economic needs and the use of computers can help students to become educated;
- Portuguese teachers have very little support, resources and training in web security and personal data protection. Because of this, they have lack of confidence, resistance to change and lack of access to reliable resources to these subjects;
- The lack of technical support is also an issue because without both good technical supports in the classroom and whole-school resources, teachers cannot be expected to overcome the barriers regarding the lack of knowledge related to web security and personal data protection.

Therefore, educators, teachers, the government and schools need to collaborate to overcome the barriers because the teaching of web security and personal data protection in classes varies from curriculum to curriculum, place to place and depends on several factors. Additionally, teachers need to be open minded towards new ways of teaching, prepare themselves by self-training and self-research.

## 7.4. SPAIN

A critical analysis will be developed focusing on the following issues:

- **To what extent have educational systems been adapted to the changing needs of the web security?**
- **Barriers faced by each country in the field of education and web security.**
- **Comparative analysis with partner countries.**
- **You can focus on the topic web security and personal data protection separately, because we suppose that the personal data protection is more implemented in the educational systems than web security.**

Future education system will be unleashed with the advent of a standardized rapid courseware-builder and a single point global distribution system. There are many ways to talk about the rapid growth of information that we have experienced over the past few years. But it is important to pay attention to the changing dimensions of information as well as the sheer volume of it.

The National Security Framework has been updated by means of the Royal Decree 951/2015 to strengthen the protection of government against cyber threats by adapting to rapidly changing technologies, the experience acquired from its implementation and to the European regulatory context.

In October 2015, the Ministry of Education published the Digital School Student Records that is a database model for school student records aiming to support the interoperability of software solutions. It has been developed by an agency helping schools with an implementation of ICT solutions - the National Institute of Educational Technologies and Teacher Training. The digital student records includes information in regard to student identification, educational profile, educational achievements, and other related data. The model is available to the educational institutes and governmental organisations.

Spain's 2017 National Security Strategy was approved by the Government on 1 December 2017. The National Security Council was the body responsible for defining this strategy. The following bodies participated in the process: The Ministry of Foreign Affairs and Cooperation; the Ministry of Justice; the Ministry of Defence; the Ministry of the Treasury and of the Civil Service; the Ministry of the Interior; the Ministry of Infrastructure; the Ministry of Education, Culture and Sport; the Ministry of Employment and Social Security; the Ministry of Energy, Tourism and the Digital Agenda; the Ministry of Agriculture and Fisheries, Food and the Environment; the Ministry of the Presidency and for the Territorial Administrations; the Ministry of the Economy, Industry and Competitiveness; the Ministry of Health, Social Services and Equality; and the

National Intelligence Centre. The Strategy also includes contributions from the independent Advisory Committee, comprising more than 50 experts, including distinguished academics from all over Spain, think-tank analysts, private sector representatives, and members of associations related to the national security areas included in this document.

According to the present Spanish Educational Law, ICT competence involves the creative, critical and secure use of information and communications technologies to achieve objectives related to work, employability, learning, use of free time, promote inclusion and participation in the society.

The hyperconnectivity of today's world exacerbates some of the security system's vulnerabilities and requires greater protection of networks and systems, as well as the public's privacy and digital rights. Spain must adapt to this permanent transformation by stepping up its efforts to digitalize and technify the State and society, based on an educational and training system adapted to this new reality. In this context, Spain must foster a culture of national security, supported primarily by a comprehensive educational system, which strengthens awareness of the prevailing threats and challenges, and their possible impact on the way of life and the prosperity of the Spanish people. Effective national security requires both social awareness among citizens and the participation of their representatives.

INCIBE and Internet Segura for Kids (IS4K) released a project co-financed by the European Union (EU) through the financing program CEF-Telecom, Safer Internet (2015-CEF-TC-2015-1). The specific objective is to set up and to continue supporting generic services provided by Safer Internet Centres (SICs) in all EU Member States, building on their interoperability with the EU core platform and its services. The SICs will maintain and expand national platforms to run a range of safer internet services providing:

- An awareness centre for empowering children, parents and teachers to make the best use of the Internet, building on enhanced digital resource centres (repositories), from which specific awareness toolkits and services will be adapted and deployed, in cooperation with third parties (schools, industry).
- Online helpline services for reporting and dealing with harmful contact (e.g. grooming, online abuse), conduct (e.g. cyberbullying, hate speech, sexting) and content online.
- A hotline for receiving and managing reports and data on online illegal child sexual abuse material.

The main benefits of this project are:

- The awareness of society with campaigns on the safe use of the Internet by children.

- The free and confidential Helpline service where anyone can contact if you are concerned about something related to the Internet.
- The reporting line where citizens can report the content of child sexual abuse that you find on the network.

The main objective of the Project is the promotion of the safe and responsible use of Internet and new technologies among children and adolescents, through the establishment of the Spanish Sefer Internet Centre, which will carry out the following tasks:

- Awareness and train minors, young people, families, educators and professionals in the area of the child, through the development of campaigns, initiatives and nationwide programs.
- Offer a helpline service to advise and assist minors, families, educators and professionals in the area of the child on how to deal with Internet risks: harmful content, harmful contacts and inappropriate behavior.
- Organise the Safer Internet Day in Spain.
- Reduce the availability of criminal content on the Internet, mainly child sexual abuse, by supporting the FCSE.

As schools are classified as a public authority for the purposes of data protection and GDPR, they must assign a Data Protection Officer who is solely responsible for any data protection and compliance with the GDPR regulation. It is important to consider where this role will sit in line with the school's structure and governance arrangements.

It is therefore cruzial to sensitize the children about the practices that could be followed, providing:

- A digital education from a very early age in order to face the possible threats when using the Internet.
- Protecting measures in their devices to ensure children's privacy and protection.
- Files and documents must also be controlled and protected by using passwords or additional encryption systems
- Children's trust must be increased and this will increase their confidence regarding any security incident.
- Schools are spaces that we must ensure against the threats that arise through the use of the Internet.

A specific training about computer safety and security for them is already fundamental in a world that is moving towards digital.

# BIBLIOGRAPHY

Bundesministerium für Bildung, Wissenschaft und Forschung[1] (2019). Berufsbildende Schulen in Österreich. Downloads. Retrieved from: https://www.abc.berufsbildendeschulen.at/downloads/.

Bundesministerium für Bildung, Wissenschaft und Forschung[2] (2019). Digitale Bildung. Masterplan für die Digitalisierung im Bildungswesen. Retrieved from: https://bildung.bmbwf.gv.at/schulen/schule40/index.html.

Federal Chancellery of the Republic of Austria (2013). Austrian Cyber Security Strategy. Retrieved from: https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

FH Campus Wien (2019). IT-Security. Retrieved from: https://www.fh-campuswien.ac.at/studium/studien-und-weiterbildungsangebot/detail/it-security-master.html?tx_asfhcw_course%5Bcontroller%5D=Course&cHash=a18489cd90dc46365309 43c1555dcd9a.

FH Oberösterreich (2019). Sichere Informationssysteme. Masterstudium Vollzeit. Retrieved from: https://www.fh-ooe.at/campus-hagenberg/studiengaenge/master/sichere-informationssysteme/.

Saferinternet.at[1] (2019). Digitale Grundbildung Sek1. Retrived from: https://www.saferinternet.at/zielgruppen/lehrende/digitale-grundbildung-sek1/.

Saferinternet.at[2] (2019). Services. Retrieved from: https://www.saferinternet.at/services/.

Saferinternet.at[3] (2019). Neuer Onlinekurs für Lehrende! Retrieved from: https://www.saferinternet.at/news-detail/der-saferinternet-at-onlinekurs-fuer-lehrende-geht-in-die-zweite-runde/.

Saferinternet.at (2018). Aktivitäten, Angebote & Erfolge seit 2005. Retrieved from: https://www.saferinternet.at/ueber-saferinternetat/die-initiative/?file=2516.

Universität Wien (2019). Kursprogramm. Retrieved from: https://www.univie.ac.at/kursdatenbank/kursreferat.html.