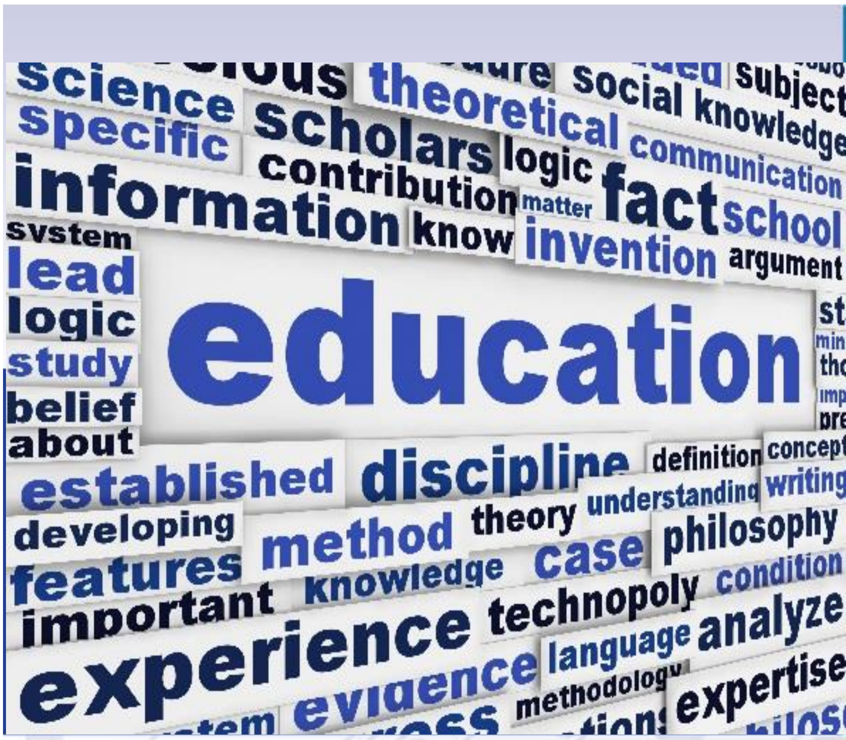


Status of privacy and NIS course curricula in Member States

PUBLISHED

EDUCATION

OCTOBER 2015

www.enisa.europa.eu

European Union Agency For Network And Information Security

[Left intentionally blank]

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Philip ANDERSON, CEI expert, Northumbria University, Newcastle upon Tyne (UK)

Stefano DE PAOLI, CEI expert, Abertay University, Dundee (UK)

Daria CĂTĂLUI, ENISA (EU)

For enquiries on EDUCATION refer to Daria CĂTĂLUI, editor of this report.

Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-127-4
DOI: 10.2824/402788

Table of Contents

1. Executive summary

User Education is key in cyber security. Our work for this report follows up on previous efforts and suggested recommendations from 2014 and 2013. The first objective of this report is to identify gaps between available training courses, certifications and NIS education needs with particular emphasis on ePrivacy. The second objective is to suggest further actions based on the analysed needs of NIS communities in Europe.

From the desktop research, the focus for most of the courses that included privacy appeared to be in the computer science, computer security, information security, and cybercrime and cyber security subject areas. However there were a number of courses that included privacy law (Information Technology, Commercial, Corporate, Communications and Property), marketing and ethics. For several reasons, it may be that privacy is an area that relatively lately is gathering attention (compared to Network and Information Security). However this idea would require further future research to be proved. In terms of existing Massive Open Online Courses- MOOCs, the offer around the subject of Privacy and Data Protection is limited in general and there is a particular lack of MOOCs in the European context, both in terms of delivery by European Universities/Institutes and also covering Privacy and Data Protection Legislations and debates at European Levels. Furthermore, MOOCs and serious games are a path which is being explored as a practical way to transfer knowledge, support learning, raise awareness, offer professional training and unveil controversial issues and practices surrounding Privacy and Data Protection.

We developed a final section where we address recommendations to EU level organisations (e.g. University Networks, Users' Coalitions and Multipliers, Education institutions) and also Member State level organisations (e.g. Education institutions, NGOs, think tanks, Government). Among those we mention:

1. Consider exploring serious games not only for raising awareness but also as a training ground for first-responders and other professionals.
2. The report has highlighted that Privacy does not seem to feature in titles of undergraduate degree courses and further research would be required to understand why.
3. Consider to invest in MOOCs with a NIS focus, in particular addressing the issue of privacy-by-design and European Legislation. We highlighted that some of the existing MOOCs are available in national languages, this is clearly an advantage and a best practice. The report has highlighted that there is scope for some specific MOOCs relating with issues currently debated at a European Level. There is a general lack of Privacy and Data Protection MOOCs in the EU context, however this delivery opportunity could be better exploited also via existing supported platforms (i.e. OpenUpEd and EMMA).
4. Consider promoting the creation of multiple such quizzes using as basis the ENISA quiz in order to raise awareness by participating in the spread of general quizzes and awareness month.

At the same time, ENISA has further developed a quiz to test user's knowledge in Network and Information Security[1] and to disseminate good practices and knowledge from all its reports. The version 1.0 will use a better gamified approach. A relevant addition to this year quiz are Cyber Security Month badges (following the model from serious games) that are awarded upon completion of the quiz. The use of badges is also

[1] https://cybersecuritymonth.eu/references/quiz-demonstration

one of the measures adopted for supporting the full completion of the quiz by a larger number of participants.

2. Introduction

2.1 Description of the work

Previous reports[2] published by the Agency on the broader subject of Network and Information Security (NIS) Education emphasised the need to provide and support a continuous brokerage between public-private stakeholders. This report further contributes to the achievement of this objective and is the result of this year's interactions between experts and of a thorough desktop research and analysis. The report discusses some of the trends and possible implementation solutions to current NIS issues with emphasis in areas of work where ENISA has been active for a number of years and also where established collaborations with the academic community exist. In particular, this report introduces data protection concepts, places emphasis on the topic of ePrivacy[3] and builds on some of the results contained in the report Roadmap for *NIS education programmes in Europe*[4] published in 2014.

At the same time, following activities started in 2014, ENISA has further developed a quiz to test users' knowledge in Network and Information Security and to disseminate good practices and knowledge. The new quiz builds upon a pilot published in 2014 in conjunction with the European Cyber Security Month and on the feedback received from the users who participated and completed the pilot. This report describes some of the results achieved with the pilot and offers a description of the new quiz.

2.1.1 Objectives

The first objective of this report is to identify gaps between available training courses, certifications and NIS education needs with particular emphasis on ePrivacy. The second objective is to suggest further actions based on the analysed needs of NIS communities in Europe. ENISA will use its existing NIS education communities to disseminate this work.

User Education is key in cyber security as shown by Digital Agenda Scoreboard and acknowledged in many cyber security strategies of member states. Our work follows up every year on previous efforts and suggested recommendations.

2.1.2 Target

Using an approach successfully tested in previous years, this report and the research work that underpins it, has been prepared in collaboration with educators and for educators. The primary target audience for the report is represented by educators and policy-makers in the field of NIS education. The Agency's NIS education communities include not only IT administrators and professionals but a larger audience, including training and education providers of multi-disciplinary backgrounds.

[2] See http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/nis-in-education-reports
[3] More about ePrivacy directive http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
[4] See http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe

3. Policy review

3.1 EU Digital Agenda Member States' scoreboards

Before presenting the findings of the research conducted in the area of NIS Education – with a focus on ePrivacy – it is important to make a contextual introduction. The introduction in this paragraph and the next (3.2) will support a better reading of the research and analysis work conducted for this report.

The Internet and Information Technologies have become a defining component of our societies and have inevitably played a role in many processes of social change. Already in the seventies of the last century, scholars raised attention to emerging forms of social arrangements broadly defined as *Post-Modern Society*[5]*, Knowledge Society* or *Information Society*[6]. These are societies characterised by the production of symbolic rather than material output, by an increased capacity to produce and process information and by the ability to use information to take further decisions and introduce further reflexive changes. Other authors, especially in the nineties of last century coined the term *Network Society*[7] which emphasises – in addition to the capacity to generate and use information – the pervasive role that networks have on social organisation. One such network is clearly the Internet. While some of these concepts have also been criticised in more recent years[8], it remains true that Information Technologies, Mobile technologies and the Internet, play nowadays a prominent role in social organisation. They provide positive aspects for social change – think for example about the increase of communication possibilities – but also introduce new challenges and inequalities, including those related with the skills and competencies that are necessary to live and work in the knowledge society. For example it is not uncommon to hear about the skills gap in the ICT industry in Europe, with the industry absorbing annually more personnel than the EU education system can produce[9]. These changes also call for the need of new abilities, not just in term of work or professional competencies but also for leisure and ordinary life more general. For instance – touching upon issues recently addressed in ENISA reports - the advent of the Internet of Things and the development of the smart home concept, will require home inhabitants to be able to master and control new technologies and use mobile devices to control and manage their houses. At the same time these changes require inhabitants to pay attention to security issues, for instance related with their ePrivacy and with the ability to protect their behaviour and personal data[10].

A useful concept to introduce at this point is that of *e-skills*. According to the document *e-Skills for the 21st Century: "Overview, Key Definitions and Strategy"*[11] published by the European Commission this term encompasses *" a broad set of skills necessary in the modern workplace and digital economy. Successful*

[5] Touraine, A. (1988). *Return of the Actor Social Theory in Postindustrial Society*. Minneapolis: University of Minnesota Press.
[6] Bell, D. (1976, May). The coming of the post-industrial society. In *The Educational Forum* (Vol. 40, No. 4, pp. 574-579).
[7] Castells, M. (2000). *The information age: economy, society and culture. Vol. 1, The rise of the network society* (Vol. 1). Oxford: Blackwell.
[8] See for instance Fuchs, C. (2007). *Internet and society: Social theory in the information age*. Routledge.
[9] See http://eskills-vision.eu/about/e-skills-gap/
[10] See https://www.enisa.europa.eu/media/press-releases/are-smart-homes-cyber-security-smart
[11] See European Commission http://ec.europa.eu/DocsRoom/documents/7146

innovation in ICT requires cross-disciplinary, cognitive and problem-solving skills as well as an understanding of the fundamentals of business and communication skills, including competence in foreign languages. They should be seen in the wider context of a core set of competences equipping all European citizens for a knowledge-based society. These key competences should be provided in a lifelong learning context". Education and training are key instruments to provide these e-skills and bridge any eventual skill gaps in citizens' ability to live in the Knowledge Society. This report contributes to this perspective by providing an initial map of training and education opportunities in Europe around the issues of ePrivacy. The matching between the educational offer and the job offer should be further analysed and more agile action is needed. Further to this issue, it is clear that in Europe and worldwide the digitalisation has represented a disrupter for business as usual. All business sectors have taken on board new technologies and new ways of organising work and have become part of the digital economy. For example, according to the statistical data that can be consulted in the Digital Agenda[12] scoreboard 2015, between 2001 and 2011 digitalisation accounted for 30% of GDP growth in the EU. The data shows that all EU Countries are moving forward toward a digital economy and society, however they also show some differences of speed among member states. Furthermore, for future development the digital single market package was introduced in May 2015 and it will be evaluated against its three pillars: (1) better access for consumers and businesses to digital goods and services across Europe; (2) creating the right conditions and a level playing field for digital networks and innovative services to flourish; (3) maximising the growth potential of the digital economy. In particular a composite index has been introduced for the measuring the results of the digital agenda objectives: The Digital Economy and Society Index (DESI).

The DESI is organised around six key dimensions: 1.Connectivity; 2.Human capital; 3. Use of internet 4.Integration of digital technology; 5. Digital public services; 6. Research and Development (R&D). We recommend the use of the index to understand the progress of each country in the EU or as general overview. In particular, according to the set roadmap the Human Capital dimension "*measures the skills needed to take advantage of the possibilities offered by a digital society. Such skills go from basic user skills that enable individuals to interact online and consume digital goods and services, to advanced skills that empower the workforce to take advantage of technology for enhanced productivity and economic growth*". In this report we conduct an analysis of the existing training and education offer in terms of ePrivacy curricula that offer opportunities to improve the Human Capital dimensions.

Privacy is a concept that needs to be approached holistically and with an interdisciplinary perspective as the concept is in various ways tied with social, economic, legal, political and technical aspects[13]. The multifaceted nature or Privacy clearly calls for an interdisciplinary approach to Privacy[14] also in terms of training and education. In the following pages various possibilities offered by Education bodies and actors in Europe and across diverse disciplines are presented and discussed.

[12] See http://ec.europa.eu/digital-agenda/en/digital-economy-and-society-index-desi

[13] Clarke, R. (2006, July). What's privacy? Available here: http://www.rogerclarke.com/DV/Privacy.html

[14] Buchmann, J. (2014). *Internet Privacy: Options for adequate realisation*. Springer Science & Business Media.

3.2 International Privacy Resources

A further introductory aspect needs to be discussed before approaching the research and analysis of training and education opportunities: the international nature of Privacy and the challenges that thinking about privacy on a global scale can bring. Privacy is a “local” concept when considered, for example according to the definition provided before, as the right for a *personal space* that an individual has. However Information Technologies and the Internet make privacy also a *global* issue for citizens, at least they need to think about their action also from a global perspective. When one considers for instance the volume of personally identifiable information that is stored or shared online it is clear that this has led to challenges when addressing the issues of privacy and security in a global landscape. Posting personal information to Facebook, updating a LinkedIn profile or storing documents on a cloud service such as Hubic/Dropbox are simple actions that many citizens do these days. These actions have obvious privacy implications, who can see the information, where this is stored or what legislation regulates the relationship between the user and the service provider. For example when an individual uses cloud providers to store data, this data will be stored somewhere – likely in a country different from that of the individual - and beside the privacy associated with the data in itself, also the location of this data and the location of the service providers will become an issue. Considering further that there is a relevant imbalance between “data processing entities, which determine what and how data is processed, and the individuals whose data is at stake”[15], this makes the issue even more relevant for individuals. It is therefore more and more important to understand data privacy, legal or regulatory demands in this global landscape.

“The UK and EU research reveals that concerns about privacy and the protection of personal data are increasingly of importance to the public.” [16] In the current situation of individual’s digital data being stored and shared, the question has to be asked “*are citizens aware of what legislation protects them when it comes to data privacy*”. In a report written by the UK Information Commissioners Office for the European Conference for Data Protection Authorities it states that “*The public need to be empowered by DPAs to understand what their rights are, how to use them and what they should expect from organisations*.” [17] Perhaps a programme of education and awareness for individual’s explaining both what data they are potentially sharing online with what they do on a day to day basis but also what are their rights to privacy in this digital age will help shape how companies use personal data that is potentially available to them.

[15] See a discussion in http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

[16] Information Commissioners Office - Data protection rights: What the public want and what the public want from Data Protection Authorities (2015) https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf

[17] See https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf

Users have the same rights online as they have offline; they should be aware of their rights. National Data Protection Authorities are there to support users.

> *"Everyone has the right to the protection of personal data concerning them" - art 16, The Treaty of Lisbon*

In light of these there are numerous (online) resources available that document and explain all of the different international privacy provisions. These can be consulted by citizens, professionals or businesses as they offer - on occasions - useful comparisons but also overviews and discussion about different regulations and standards across the globe. While most of the existing resources are quite legalistic and technical in nature, occasionally it is possible to find also simple and informative resources that ordinary citizens can consults. A possible recommendation would be to try producing more of the simple and informative tools for citizens, in this way easing the opportunities for individuals to gather knowledge and be better informed about their own privacy. Below are some examples of existing resources that are briefly discussed.

European Level

The European Data Protection Supervisor (EDPS) works to ensure that European institutions and bodies respect the right to privacy when they process personal data and develop new policies. The EDPS monitors the processing of personal data in the EU administration and ensures compliance with the data protection rules and advises the European Commission, the European Parliament and the Council on proposals for new legislation and a wide range of other issues having an impact on data protection[18]. More information regarding data protection legislation in Europe can be found on the website[19]. An interesting instrument offered by the EDPS is a comprehensive glossary of terms[20], which contains a number of terms relating to the protection of personal data, especially in the context of the EU and its institutions. The glossary is intended to support a better understanding of the activities of the EDPS and of data protection issues in a more general context. This is a good example of an easy to use resources that can be consulted to get relevant definitions and some contextualisation about relevant terms.

International Level

The Electronic Frontier Foundation (EFF) is a non-profit organization defending civil liberties in the digital world and focuses much of its activities on privacy and freedom of expression[21]. On its website the EFF has compiled a comprehensive and detailed list of international accords on privacy and data protection. The accords serve as the foundation for national laws, policy frameworks, and international agreements throughout the world[22]. This web page offers in particular a detailed list of links (URL) and it is of ease of access and brings together in one single location the key relevant international accords. On their website under 'Our Work', although not relevant to everyone, they explain in detail a number of significant legal

[18] See https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Membersmission ;
[19] See https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Legislation
[20] See https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary
[21] See https://www.eff.org/about
[22] See https://www.eff.org/issues/international-privacy-standards

cases around keys issues of privacy. A section on the same page also lists a number of whitepapers[23] published from 2005 up until 2015 discussing the challenges of data privacy.

Another organisation as a source for useful references is Privacy International, a registered UK charity that campaigns at an international level on privacy issues, have produced in collaboration with academic institutions across the globe, a number of reports in collaboration with academic institutions that document global privacy issues[24]. While the reports might not be of immediate ease to consult for citizens, Privacy International also hosts on its website a section called Privacy 101[25] which contains a collection of articles and multimedia material that, according to Privacy International tell "*everything you need to know about how these issues affect your life*".

The American Institute of Certified Public Accountants (AICPA) hosts on its website an easy to consult table that "*presents a comparison of privacy concepts set out in some domestic and international privacy regulations, laws, and guidelines in relation to Generally Accepted Privacy Principles*"[26]. While the table does not go in depth with the analysis, it is a useful resource as it offer a synthetic comparative view according to "Generally Accepted Privacy Principles".

Furthermore, a number of reports have been compiled by different international companies that detail international agreements and national laws related to privacy. Baker Hostetler, a US law firm, produced the 2015 International Compendium of Data Privacy Laws[27] . This compendium is meant as a reference guide that outlines the basic requirements in 40 countries. It is a well organised document were the countries are listed alphabetically and for each country it is broken down in to different sections, these sections are 'Applicable Law', 'Data Protection Authority and Registration Requirements', 'Protected Personal Data, 'Data Collection and Processing', 'Data Transfer', 'Data Security', 'Breach Notification', 'Other Considerations' and 'Enforcements and Penalties'. These sections are the same for all of the countries in the compendium detailing relevant information for that country. The Applicable Law section is self-explanatory in that the document lists the name of the legislation and where possible includes a URL link (most cases governmental) as a further resource and in which year it was enacted. Similarly the Data Protection Authority and Registration Requirements section names the authority for that country and outlines the requirements of registration for data processing. The countries definition of personal data and also what they see as data collection and processing as well as data transfer is given in the Protected Personal Data, 'Data Collection and Processing section. The Data Security section includes information on what data security measures are required (if any) and if a breach occurs. Finally the Enforcement and Penalties section details the sanctions that can be imposed for any breach of the legislation.

DLA Piper produced a Data Protection Laws of the World Handbook[28] and an interactive map detailing data protection laws by country[29]. The Handbook "sets out an overview of the key privacy and data protection

[23] See https://www.eff.org/wp
[24] See https://privacyinternational.org/?q=reports
[25] See https://privacyinternational.org/?q=privacy-101
[26] See http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/InternationalPrivacyConcepts.aspx
[27] See http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf
[28] See http://dlapiperdataprotection.com/#handbook/
[29] See http://dlapiperdataprotection.com/#handbook/world-map-section

laws and regulations across 77 different jurisdictions and offers a primer to businesses as they consider this complex and increasingly important area of compliance". However of particular interest for this report is the interactive map[30], which constitutes an easy to use and easy to consult instrument. Essentially the map translates the findings of the Handbook in an interactive tool. The map offers the opportunity to compare laws and regulations between countries and the comparison can be obtained around general topics (i.e. Definitions, Authorities) but also around more specific and targeted topics (e.g. Privacy Offices, Online Privacy).

While the list of resources provided here is not exhaustive but it does provide examples of some easy to use tools and resources related with Privacy in a global perspective. There are a number of websites that strongly support an individual's right to privacy in today's digital and global environment, the Electronic Frontier Foundation and Privacy International are advocates of this and contribute to the latest research around current and future data privacy issues. The handbook by DLA Piper and the compendium by Baker Hostetler are useful reference materials to gain an understanding into what countries have in the way of legislation and requirements to deal with data privacy. This gives some indication that a large number of countries take an individual's data privacy and organisations data processing responsibilities seriously.

In the following section (Section 4) of the report we offer now a preliminary analysis of existing training opportunities around Privacy and Data Protection in the European context.

[30] http://dlapiperdataprotection.com/#handbook/world-map-section

4. Status of NIS courses in EU[31]

4.1 Privacy and data protection

Education and Training

We conducted a desktop research in English in order to identify what are the current offers in terms of education and training within Member States. Some preliminary findings show however that in Europe the situation appears fragmented and there is little reference to privacy and data protection in any course syllabi although a limited number of university degrees (mainly at postgraduate level) have "privacy" explicitly mentioned in the title.

Primary education

As an example and an indication of what education around privacy is being taught and to investigate one particular country in depth the education provision in the UK from the age of 14 was chosen as one of the authors has knowledge of the different levels of the educational system. Schools in the UK can currently offer GCSE Computing which children start at 14 and sit exams at 16 followed by AS and A Level Computing which children study from the age of 16 to 18. The syllabus for both GCSE and GCE AS and A Level Computing was reviewed for particular reference to privacy and data protection. Within the GCSE syllabus written by OCR and published in September 2011[32] it was found that the word privacy appears only once in the entire document. Privacy is discussed under a section entitled 'Spiritual, moral, ethical, social, legislative, economic and cultural issues' and is placed into context with the explanation that this 'encourages candidates to explore the spiritual, moral, ethical, social, legislative, and cultural aspects of the introduction of computer-based solutions to problems through a study of their effects on society' and data protection'. For the term data protection, there was no reference to this as a phrase, however protection is mentioned and is in a section entitled Software which discuss computer security and states candidates should be able 'describe the purpose and use of common utility programs for computer security (antivirus, spyware protection and firewalls)'.

With results for privacy and data protection low a widening of the review to include other terms was looked into, security was chosen and again a small results. It would appear that the focus of the GCSE syllabus as explained out in the 'Aims and learning outcomes' is on the functional aspects of computing such as developing computer programs to solve problems. A review of the GCE AS and A Level syllabus[33] written by AQA and published in February 2015 for the terms privacy and data protection found that there was no reference to either, a review of the term security found a number of entries based around the subject of encryption and in particular different types of encryption. As with the GCSE Computing syllabus there is a strong focus on the functional aspects of computing such as programming but also networking and databases are included. Although the results seem clear for the UK regarding the issues around teaching privacy in the formal context of a syllabus further investigation should look at wider aspects that include privacy, e.g. online safety that is currently taught in schools will cover certain aspects of privacy but in a different context. There are clear limitations with only using one country and it would be a

[31] Based on a desktop research
[32] OCR. (2011) GCSE in Computing J275 at http://www.ocr.org.uk/images/81949-specification.pdf
[33] AQA. (2015) GCE AS and A Level Specification Computing at http://filestore.aqa.org.uk/subjects/specifications/alevel/AQA-2510-W-SP-14.PDF

recommendation that a detailed examination of all Member States be carried out to the same level in order to provider clearer and more comparable data.

University education

A desktop research was undertaken to identify the number of University courses but also the subject area of University courses that included the term privacy in either the title or course description, information available in English. From the desktop it was clear that within the UK using the Universities and Colleges Admissions (UCAS) website[34], which is a central organisation through which applications are processed for entry to higher education, there are no undergraduate degrees (Bachelors) that have privacy in the title. A further desktop research across a number of equivalent or similar European resources[35] appears to reflect the same findings. It should be noted that by no means was this an exhaustive search as each course listed may have a module that discusses privacy or an aspect of privacy but that was not immediately obvious and further detailed, investigation would take a significant amount of time which would be outside of this projects timescale[36].

There is however a significant shift in results when it comes to postgraduate programmes in that there are a number of courses that have privacy in the title or make specific reference to it in a description of the course (see below). It appears more common that privacy is included within other degrees (e.g. information security, informatics). In the UK the Information Security and Privacy Masters from the University of Cardiff was found to be the only course which included privacy in the title, however upon further reading of the course descriptions/aims of the courses found it was clear that privacy was included as an element within the degree. The focus for most of the courses that included privacy appeared to be in the computer science, computer security, information security and cybercrime/cyber security subject area. However there were a number of courses that included privacy law (Information Technology, Commercial, Corporate, Communications and Property), marketing and ethics.

Table 1 with Examples:

TITLE	UNIVERSITY	AIM (FROM WEBSITE)	URL
Information Security & Privacy (MSc)[37]	University of Cardiff (UK)	Appropriate security measures are an essential part of any modern enterprise. A detailed understanding of the key threats and the essential techniques for ensuring security, privacy and trust are fundamental requirements for successful information systems. Emerging software deployment and use, through the use of data outsourcing such as in Cloud computing and with the increasing use of social media platforms, opens up significant security and privacy issues which future IT professionals need to be aware of. Professionals in this field are well placed for a wide variety of employment opportunities.	http://courses.cardiff.ac.uk/postgraduate/course/detail/p148.html

[34] See UCAS website https://www.ucas.com/
[35] See http://www.prospects.ac.uk/search_courses_results.htm?t=srs&criteria.keyword=privacy&addfilter=2022
[36] Some individual privacy courses are presented in the Network and Information Security courses in Europe Map available here https://cybersecuritymonth.eu/references/universities
[37] Offers on-campus IAPP Certified Information Privacy Professional (CIPP) certification exams to students in its program.

Computer Security (MSc)	Radboud University Nijmegen (Netherlands)	Computer security is a topic of growing importance, as ICT affects ever more aspects of our daily lives Businesses and government rely on ICT to an ever larger degree. Both assessing the security of existing ICT solutions and developing more secure solutions for the future pose major scientific and societal challenges. This Master track covers a broad range of topics that is important for computer security. This includes topics in computer science (software, computer networks, and hardware, esp. smart-cards and RFID), but also mathematical aspects (cryptography and security protocols), as well as organizational and management issues, legal aspects, and societal issues (in particular privacy).	http://www.ru.nl/english/edueducat/masters/computing-security/
Security and Privacy	EIT Labs	The programme in Security and Privacy focuses on the study of the design, development and evaluation of secure computer systems, which are also capable of ensuring privacy for future ICT systems. It follows a constructive security approach to teach the very complex and challenging field of information assurance. The aim is to provide students with an understanding of the concepts and technologies for achieving confidentiality, integrity, authenticity, and privacy protection for information processed across networks.	http://www.masterschool.eitictlabs.eu/programmes/sap/

One thing that came out of the desktop search and is worth mentioning is the opportunity for students at postgraduate level to study in other European countries (via the European Institute of Technology – EIT), for example there is a Master in Security and Privacy at the Saarland University in cooperation with Technische Universität Berlin in Germany and University of Trento in Italy.

With regard to the outcomes of the desktop findings something else worth noting is that looking at the titles and course descriptions it would appear that privacy is the smaller component rather than major focus of the programme, e.g. Computer Security and Privacy in which computer security makes up a significant part of the programme syllabus. The variety of postgraduate educational courses available that have privacy in the title or mention privacy in the course description perhaps reflects the wider relevance and application of privacy as a subject. As to why it would seem that privacy only appears in postgraduate or doctoral courses may suggest an industry requirement, for example people looking to progress their careers were privacy is key or there is a need for further and continuing research in this dynamic subject area. Another possible factor may be that privacy is an area that relatively lately (compared to NIS) is gathering attention. Hence is somehow natural that the introduction of privacy into these courses is still at an early stage. However this suggestion would require further research to be proved. Within a University undergraduate course where you would expect the inclusion of privacy in a given subject area such as computing, computer security or law it would likely be present but the level of detail necessary to discover that from simply browsing University course pages may not be sufficient. Another issue to bear in mind is that simply searching for University degree titles may be somewhat flawed, from a marketing perspective undergraduate course titles need to be attractive and capture the interest of potential students from the age of 14 – 18 to influence their choice therefore offering a broader area and focused titles that students clearly understand is necessary. It could simply be that privacy is not an attractive term to use in a degree title or the fact that potential students may not have a clear understanding of what it means.

4.1.1 Professional education, Training and Certifications

Beyond University and Higher Education, there are a number of opportunities to obtain training on Privacy and Data protection, aimed both at professionals working in various sectors (e.g. healthcare, education), at entrepreneurs and also for the general public. We conducted an initial survey of existing opportunities via a desktop research based on English keywords. Some opportunities present in MS' have been identified and some of the most relevant examples are briefly discussed and analysed in this section.

Of particular interest for professionals working directly in the area of privacy (e.g. Data and Privacy officers/managers) are the Privacy Training Classes and Online Training[38] offered by the International Association of Privacy Professionals (IAPP). The IAPP is a not-for-profit organization that helps define, support and improve the privacy profession globally and is the largest information privacy organization in the world[39]. The IAPP training is offered both face-to-face and online. While the IAPP operates globally, face-to-face training is offered also across Member States. These trainings are also offered in the perspective of preparing privacy professional in obtaining the IAPP privacy certifications: CIPP (for the area of Law and Regulations), CIPM (for operations) and CIPT (for the technologies)[40]. Of particular interest for the European context are the following courses:

- *Foundation*[41], which is the foundational training for preparation for the certificate tests.
- *Privacy in Technologies*[42] (CIPT) which covers essential aspect of privacy in relation with IT (e.g. Online Privacy, Systems Applications and Cloud Computing).
- *Privacy Management*[43] (CIPM) with a focus on business operations and privacy.
- *European Privacy* (CIPP/E) which cover essential aspect of for the European Context such as the Data Protection Regulations and its compliance.

The certifications offered by the IAPP are also considered relevant in the European DPO[44] position paper *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001*[45], which states that "*The possession of such a certification should be considered as an asset by EU institutions/bodies when selecting their DPO*"[46].

[38] See https://privacyassociation.org/learn/training-classes
[39] See https://privacyassociation.org/
[40] See IAPP certification descriptions at https://privacyassociation.org/certify/programs
[41] See https://privacyassociation.org/media/pdf/certification/course-outlines/FoundationCourseOutline.pdf
[42] See https://privacyassociation.org/media/pdf/certification/course-outlines/CIPTCourseOutline.pdf
[43] See https://privacyassociation.org/media/pdf/certification/course-outlines/PrivacyProgramManagementCourseOutline.pdf
[44] See https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/DPO
[45] See http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf
[46] See p. 5 of the position paper, available here http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf

The ECDL Foundation is also a relevant provider of NIS training and has some opportunities in the area of Privacy and Data Protection, although not extensive. In the *Roadmap for NIS education programmes in Europe* the ECDL module on IT Security[47] was mentioned as a relevant training opportunity in the area security for the general public. The IT Security module offers also a reasonable coverage of Privacy related issues across the different areas being taught, from general concepts, to privacy online, to data protection. Indeed one of the key module goals is described as follows: *Understand the key concepts relating to the importance of secure information and data, physical security, privacy and identity theft[48].* Recently ECDL officially endorsed[49] a module developed by the Irish Computer Society (ICS) entitled Data Protection Essentials[50]. The module is described as *"relevant to all employees who handle information about clients, or members of the public who need a basic understanding of data protection rights and responsibilities"*. Core topics of the module include Fundamental definitions, Obligations, Individual rights and Regulation and enforcement[51]. In particular, the ICS has the ambition to offer the module (in its E-learning version) to over one million Irish ECDL students by 2017. Among the targeted audiences are a variety of profiles who on a daily basis deal with personal data, such as Human Resources staff, Legal secretaries or Health Sector Administrators[52]. ICS also offers a national certification *ICS Data Protection Practitioner Certificate[53]*.

In Italy, the AICA (Italian Association for Informatics and Automatic Calculus), offers an ECDL certification called *Diritto nell'ICT*[54] (ICT Law) aimed at professionals working in public administration, police, law firms, education but also aimed a citizens and students in technical and law disciplines. The certification is composed of two modules one of which is called Protection of Personal Data: Privacy and Security[55], this module has a strong focus on the evolution of the concept of privacy and the Italian privacy laws. AICA has also recently signed an agreement with Federprivacy, the Italian national association of privacy professionals[56], where Federprivacy recognises "18 credits" related to the certificate of quality of their members for those who complete the AICA module on Privacy and Data Protection.

In Poland, the Polish Information Processing Society (PTI) has developed a module called e-Urzednik (e-Clerk) for the use of ICTs in public administration. This module is ECDL endorsed. While the module offers a general perspective of the use of ICTs it also contains a section on Privacy and Data Protection, covering European and National Legislation (section 1.2.2 of the syllabus)[57]. In Germany, the ECDL national operator has developed a module called Datenschutz[58] (Data Protection) *"aimed at employees who regularly handle personal data and customer data. The initiative for the module springs in large part from the increasing need for better training in data protection"*.

[47] See ECDL IT Security Module: http://www.ecdl.org/programmes/index.jsp?p=2928&n=2944
[48] See http://www.ecdl.org/media/ITSecurity1.pdf
[49] See http://www.ecdl.org/index.jsp?p=932&n=3007&a=5318
[50] See http://www.ics-skills.ie/data-protection/essentials.php
[51] See http://www.ics-skills.ie/data-protection/essentials.php
[52] See full list here: http://www.ics-skills.ie/data-protection/essentials.php
[53] See http://www.ics-skills.ie/data-protection/practitioner-certificate.php
[54] See http://www.aicanet.it/aica/diritto-ict
[55] See syllabus http://www.aicanet.it/aica/diritto-ict/per-i-candidati/Modulo%201-Protezione%20Dati%20Personali%20Ver1-0.pdf
[56] See website http://www.federprivacy.it/
[57] See https://www.ecdl.pl/e-urzednik
[58] See http://www.ecdl.org/index.jsp?p=932&n=3007&a=5320

In the UK, the Information Commissioners Office (ICO) which is an independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals gives advice and guidance to members of the public and organisations regarding the various aspects of privacy and data protection. On the ICO website there are a number of training videos[59] for organisations that raise awareness about particular issues of data protection such data protection, privacy notices and data breaches. In the ICO's latest report, Information Commissioner's Annual Report and Financial Statements 2014/15[60], a number stated that for 2014/2015 they received just over 180,000 reports in relation to PECR (Privacy and Electronic Communications Regulation) which was an 11% increase on last year.

Also in the UK, the BCS, the Chartered Institute for IT, fosters links between industry, academia and business to promote new thinking, education and knowledge sharing[61]. As an organisation within the computing discipline they promote continuing professional development and one method is via a series of respected IT qualifications and one such certification is Data Protection[62], which they describe "*as a way to broaden your understanding of the law and its practical application. It incorporates the latest changes and updates outlined in the Data Protection Act of 1998 and the way it works with the Privacy and Electronic Communications (EC Directive) Regulations 2003*"[63].

At national level, Data Protection Officers can also act as a catalyst for training opportunities by either signalling relevant training to interested parties or by developing and offering training material. In Ireland, the Data Protection Commissioner has developed guides and multimedia materials[64]. The Commissioner website also points interested parties to training opportunities offered by third party organisations. In UK, the Information Commissioner's Office also has developed training and dissemination materials[65] as well as e-learning opportunities. Across the activities run by research projects funded by the European Commission there have been examples of training related with Privacy. For instance the FP7 Project PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in Research) held a Training Workshop this year (9-10 March 2015) on Privacy and the methodologies developed by the project[66]. The Horizon2020 Project STARTIFY7 aims at training young future ICT entrepreneurs in Europe. The project organises training "academies" and of particular interest was the Trento Summer Academy aimed at those with an entrepreneurial interest in Security and Privacy by Design[67] .

Some considerations of the findings from this analysis are as follows:

- Training activities outside University/Higher Education are often offered in conjunction with specific certifications both internationally and at national levels;
- National Computing Associations – at least in some of the cases considered here - have a fundamental role in offering training opportunities on Privacy and Data Protection;

[59] See https://ico.org.uk/for-organisations/improve-your-practices/training-videos/
[60] See https://ico.org.uk/media/about-the-ico/documents/1431982/annual-report-2014-15.pdf
[61] See http://www.bcs.org/category/5651
[62] See http://certifications.bcs.org/category/15742
[63] See http://certifications.bcs.org/upload/pdf/infosec-dp-syllabus.pdf
[64] See http://www.dataprotection.ie/docs/Training-and-Awareness/805.htm
[65] See https://ico.org.uk/for-organisations/improve-your-practices/posters-stickers-and-e-learning/
[66] See http://pripareproject.eu/events/privacy-training-workshop-3/
[67] See http://www.startify7.eu/trento

- National Computing Associations often work in conjunction with other providers, e.g. ECDL, in offering training and certifications (e.g. via endorsements);
- Training activities offered via EU research project appears to focus on bridging the gap between research and practical application of methodologies and techniques;
- Certification are relevant for professionals (e.g. Data Protection Officer) but in certain countries (e.g. UK) there are more than one;
- National Data Protection Offices have a relevant role in producing and disseminating training material.

4.1.2 MOOCs: Privacy & Data Protection

MOOC – Massive Open Online Courses are a new way of delivering online education[68]. MOOCs are often similar to university courses in terms of content and breadth, but the delivery model, the assessment and the peer collaboration is different from traditional University courses. They are often delivered by elite universities from Europe and US and hence there is the promise for top level education for a wider audience. According to existing research, MOOCs have seen so far a high level of enrolment coupled with a low level of completion[69]. The debate is still open about the effectiveness of this delivery method in comparison to traditional university teaching[70] and a recent study highlighted the merits of this approach[71]. Beside the wider debate around MOOCs, whose review is outside the scope if this report, it must be signalled that the availability of material via online platforms offer also to least engaged participants to opportunity to acquire relevant knowledge.

The ENISA report *Roadmap for NIS education programmes in Europe*, published in October 2014, did consider the current situation around MOOCs for Network and Information Security. The report stated that MOOC could constitute an interesting approach for delivering NIS Education to large audiences. The report also reviewed relevant best practices such as the Cybersecurity MOOC supported by the UK Government via the FutureLearn platform, with the goal to *"raise awareness of cyber security among a mass audience as well as providing a high quality course which will make the subject accessible to non-specialist learners".* The report also highlighted the interest of the European Commission for this method of delivering education, via for example the OpenUpEd platform[72] supported by the Long Life Learning Program. Recently another MOOC platform project – called EMMA - has been launched by the Commission[73]. Although both OpenUpEd and EMMA do not have yet MOOCs in the NIS area. The *Roadmap for NIS education programmes in Europe* also did offer a specific recommendation about MOOCs: Institutions should start to develop NIS MOOCs. In addition, any future pan-European MOOC initiatives should consider including 'NIS for ALL' modules within the programmes portfolio.

[68] See for an exhaustive review https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/240193/13-1173-maturing-of-the-mooc.pdf

[69] See for instance completion data from MIT and Stanford http://www.edtechmagazine.com/higher/article/2014/02/harvardxs-and-mitxs-mooc-data-visualized-and-mapped

[70] See for example: https://www.edx.org/blog/comparing-effectiveness-learning-moocs

[71] Colvin, K., Champaign, J., Liu, A., Zhou, Q., Fredericks, C., & Pritchard, D. (2014). Learning in an introductory physics MOOC: All cohorts learn equally, including an on-campus class. The International Review Of Research In Open And Distance Learning, 15(4). Retrieved fromhttp://www.irrodl.org/index.php/irrodl/article/view/1902/3058

[72] See http://www.openuped.eu/

[73] See http://platform.europeanmoocs.eu/

While in the area of NIS there is a sufficient number of MOOCs also taught by European Universities, the situation in relation to Privacy and Data Protection appears weaker, although there are some interesting initiatives. We conducted a recognition of the main MOOC platforms (edX, Coursera, FutureLearn, Udacity, OpenUpEd, iversity, Canvas Network) as well as one from MSs national platforms (e.g. MiriadaX in Spain) in order to map existing MOOCs offer in the area of Privacy and Data Protection[74]. The website MOOC-List has also been used for this purpose[75]. We did a search for relevant keywords (e.g. privacy, surveillance, confidentiality, data protection). The offer around the subject of Privacy and Data Protection is limited in general and there is a particular lack of MOOCs in the European context, both in term of delivery by European Universities/Institutes and also covering Privacy and Data Protection Legislations and debates at European Levels. In total we identified eleven MOOCs on Privacy and/or Data Protection either as stand-alone courses or courses that embed at least one lecture related with privacy and data protection. Of those taught in English, seven are (or were) delivered by US Universities and one each by an Australian University and a European Research Institute. Interestingly there are two additional MOOCs loosely related with Privacy and Data Protection taught in Spanish[76] and French[77] and delivered by European Institutes on national MOOCs platforms.

Some conclusions of these findings are as follows:

- There is a lack of offer around the subject of Privacy and Data protection (as a general keyword) in any relevant MOOCs platform;
- Some of the existing Courses overlap with the current debate around Mass Surveillance and the NSA/Snowden Scandal;
- Some courses are related with the issue of Big Data and Social Media and some with Data Protection in the Health Sector;
- OpenUpEd – the European Commission MOOC platform does not appear to have courses related with privacy and data protection;
- FutureLearn – the UK MOOC platform does not have courses on privacy and data protection;
- At European Level, there are some limited examples of MOOCs on Privacy and Data Protection taught in Member States languages other than English;
- Most of the existing MOOCs are taught by US based Universities (in any case EU Universities are not delivering on this subject in English);
- Given that essentially all of the generalist offer (i.e. in English) comes from United States, the type of content (in particular around legislations and technical requirements addressing legislation) does not appear suitable for European Based Learners;
- Privacy MOOCs are delivered within the scope of several different disciplines (Social Sciences, Law, Computer Security, Business & Management, Health & Society, Political Science), however courses with a NIS focus are largely underrepresented.

In general, the current situation could be much improved especially in terms of NIS education and we develop in the recommendations' section. A positive note is however the already noted existence of

[74] These MOOC are available on map at https://cybersecuritymonth.eu/references/universities
[75] See https://www.mooc-list.com/
[76] See https://www.miriadax.net/web/derecho-redes-sociales
[77] See https://www.france-universite-numerique-mooc.fr/courses/CNAM/01013/session01/about

MOOCs in languages other than English developed in Spain and France. Given that MOOCs are essentially stand-alone courses which can be delivered over a short number of weeks and that are taken by students which are other than traditional university students (often people which already have University degrees), there is scope for developing more offer in the area, also covering the different aspects of Privacy and Data Protection at social, economic, legal and technical levels.

In particular, with the increased interest in the subject of Privacy-by-Design (see for example the ENISA report *Privacy and Data Protection by Design - from policy to engineering*[78]) and the engineering of privacy in system design, it is surprising that there is no offer around this aimed at software developers and data protection officers. Perhaps a more comprehensive MOOC offer would help bridging the "*awareness and e-illiteracy gaps*" that the report *Privacy and Data Protection by Design* did identify as a major issue for the diffusion of privacy-by-design best practice in the design and implementation of software systems. Software developers and data protection officers may find in MOOCs the opportunity to acquire knowledge about privacy-by-design, while studying at their own pace.

Likewise, in the European context there has been an intense debate around Privacy and Data Protection, for instance with regard to recent initiative and events: the proposed right to Erasure, the EU Privacy Seal, the reform of the Data Protection Legislation in Europe[79], the mass-surveillance issues. These are all aspects that could feature in MOOCs aimed at Law and Social/Business experts and scholars. Currently however this offer appears non-existent for specialised areas.

Therefore, the recommendation offered by last year report around the idea of having European Institutes developing more MOOCs offer in the area of Cybersecurity, appears even more valid in the area of Privacy and Data Protection. European Institutes could also take advantage of existing European platforms and initiatives in this area such as the OpenUpEd and the EMMA platforms, both funded by the European Commission. The recommendation from last year report also insisted on "*for Beginners*" MOOCs, aimed at a wider audience, of which the already mentioned Cybersecurity MOOC sponsored by the UK government and delivered on the FutureLearn platform is an example. The non-English MOOCs (in French and Spanish) described before appear quite generalist an approach and this seems a step in the relevant direction. Of the English taught courses, one is offered as an introduction to data privacy for non-experts in particular aimed at educators (i.e. teachers) at all level[80]. However this is strongly shaped by the US context.

[78] See https://www.enisa.europa.eu/media/news-items/deciphering-the-landscape-for-privacy-by-design
[79] See http://ec.europa.eu/justice/data-protection/review/index_en.htm
[80] See https://www.canvas.net/browse/excelined/courses/data-privacy-get-schooled

4.2 Other specialized topics: Short Review of Privacy and Data Protection Quizzes and Serious Games

While traditionally games (both digital and offline) are seen as having only an entertaining goal, researchers and industry have started to explore the fusion of game-based approaches and Information Technologies for serious purposes[81]. Serious and educational games are these days used in a variety of contexts and fields that include for example promotion of well-being and rehabilitation, general education or training of professionals. The use of serious games and gamified approaches to learning constitutes an interesting path to explore also in terms of NIS education and awareness [82] [83] [84] and the creation of the NIS pilot quiz by ENISA - for the activities of the 2014 Cyber Security Month- also follows this perspective. The 2015 activities related with the quiz are described in the next section of this report. In this section of the report instead are briefly reviewed some of the existing entertaining- gamified opportunities for learning and training in the area of Privacy and Data Protection. The material presented in this section has been collected via a desktop research, during the months of May-July 2015. The review offered here does not pretend to be exhaustive, and the goal is to preliminary discuss some types of existing games, consider what are the intended audiences of these games and highlight best practices emerging from the gamified approach. More research work would eventually be required for an exhaustive and better conceptualised review on the subject of serious gaming in Privacy and Data Protection.

Serious Game is the modern tool using the front end of a game (mainly to engage the player) and a back end engine to gather useful data which could use for improving work process efficacy and expanding knowledge base[85].

Clark Abt discussion in this book Serious Games[86]: Reduced to its formal essence, a game is an activity among two or more independent decision-makers seeking to achieve their objectives in some limiting context. A more conventional definition would say that a game is a context with rules among adversaries trying to win objectives. We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement.

Across the web it is not uncommon to find quizzes or serious games in which a gamified entertaining activity is matched with goals of raising awareness, disseminate best practices and offering additional

[81] See for an overview the following publication Susi, T., Johannesson, M. & Backlund, P. (2007). *Serious games – An overview*, (Technical Report HS-IKI-TR-07-001). Retrieved from http://www.his.se/PageFiles/10481/HS-IKI-TR-07-001.pdf

[82] See for interesting examples in and outside the EU context http://www.infosecuregroup.com/CSI.html, http://itsecurity.vermont.gov/Fun_with_Security/games or http://www.carnegiecyberacademy.com/funstuff.html

[83] See a recent article on the Computer World Magazine about using gamified approaches to training in security http://www.computerworld.com/article/2489977/security0/boost-your-security-training-with-gamification-really.html

[84] See a blog post from SANS on the gamification of security awareness http://www.securingthehuman.org/blog/2012/01/17/gamifying-security-awareness

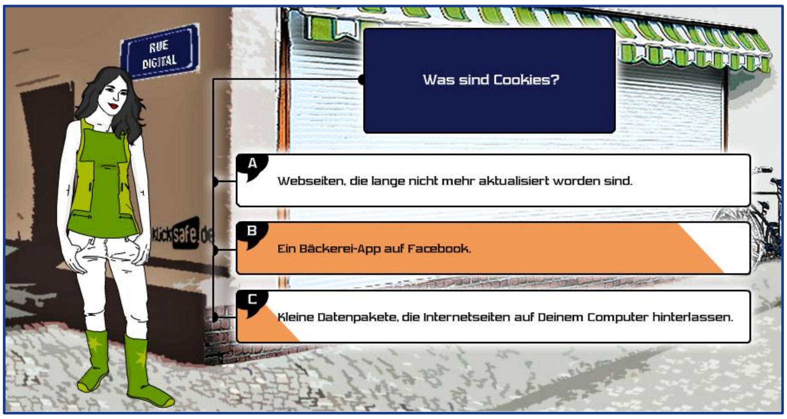
[85] http://2015conf.seriousgamesconference.org/

[86] https://en.wikipedia.org/wiki/Serious_game

training on Privacy and Data Protection. It is for example not uncommon to find quizzes about Privacy published by news and media outlets (e.g. newspapers) as a complement to articles[87] or other media initiative on the subject.

More relevant for the purpose of this brief review are examples of quizzes that have been developed by public authorities and public initiatives with the intent to raise awareness about specific aspects of, for example, current legislation, general practices and general attitudes of population. An example of a quiz developed by a public authority is the *Privacy and Data Protection Quiz*[88] of the UK Information Commissioner's Office. This quiz is an entertaining way of disseminating the results of an annual survey which is conducted by the Information Officer on 1500 respondents: the quiz offers participants the opportunity to see how their view compares to that of the general public. Another example of a quiz developed by a public authority, is a quiz on data protection created by the Data Protection Office of the Rehinland-Pfalz Land in Germany[89]. The quiz offers participants an opportunity to test their knowledge with particular emphasis on "*the Internet and social media such as Facebook*". The same public authority also offers a quiz on data protection for young people[90], where participants are asked to guide the quiz character "Ben" in his digital life and helping him making choices that are relevant for his data protection and privacy. Outside Europe a similar initiative has been presented by the Office of the Privacy Commissioner in Canada with a quiz for young people[91] and one for businesses[92]. In both these quizzes the goal is to make each participant test "*How well do you know your privacy rights?*". Another example comes from the Klicksafe[93] project co-funded by the European Union, which is an awareness campaign promoting media literacy and adequate handling of the Internet and new media. The Klicksafe project offers a number of quizzes (available only in German) relevant for young people online life, including a quiz offering tips about Privacy and Data Protection[94]. The quiz comes with an appealing graphical interface and the use of avatars to guide participants across real-life scenario situations and quiz questions.

[87] See for example http://newsquiz.sciencemag.org/privacy/, http://www.wsj.com/articles/how-much-do-you-know-about-data-privacy-1429499471, http://www.ilsole24ore.com/art/tecnologie/2014-01-29/conosci-privacy-web-072247.shtml?sondaggi, http://www.journaldunet.com/questionnaire/fiche/14520/d/f/1/
[88] See https://ico.org.uk/about-the-ico/privacy-and-data-protection-quiz/
[89] See https://datenschutzquiz.hs-kl.de/
[90] See http://www.verbraucherzentrale-rlp.de/datenschutz-quiz
[91] See https://www.priv.gc.ca/youth-jeunes/quiz/index_e.asp
[92] See https://www.priv.gc.ca/quiz/html_e.asp
[93] See http://www.klicksafe.de/
[94] See http://www.klicksafe.de/qz/quiz03/_project/



Was sind Cookies?

A Webseiten, die lange nicht mehr aktualisiert worden sind.

B Ein Bäckerei-App auf Facebook.

C Kleine Datenpakete, die Internetseiten auf Deinem Computer hinterlassen.

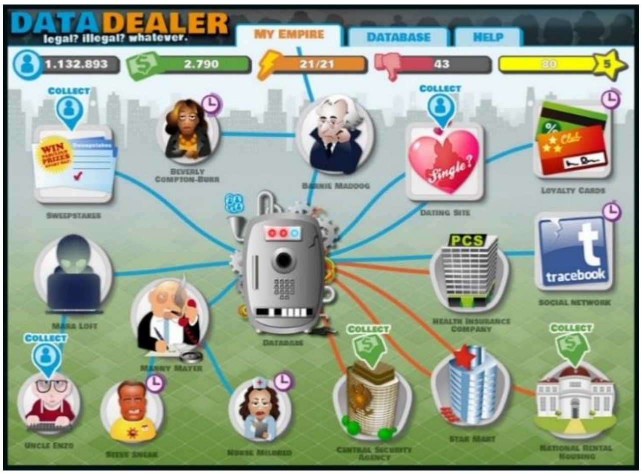
Graph 1 – Screenshot of one of the questions composing the Klicksafe.de quiz on Data Protection (Datenschutz)

These just mentioned are all examples that show the interest of public authorities in leveraging entertaining quizzes for disseminating knowledge about ePrivacy. Quizzes are created for both young people but also for other audiences, such as the general public or even companies. On the other side, the use of quizzes confirms again the important role of Privacy and Data Protection Offices and other public initiatives in offering training and learning opportunities.

Quizzes are a type of entertaining approach which offers learning opportunities leveraging a model of sequential questions & answers. There are a few known examples of other types of games (both digital and offline) related with Privacy and Data Protection aimed at schools, general audience and also professionals. While the landscape of serious gaming about Privacy and Data Protection appears quite fragmented and some of the existing games are now inactive or not used further, there are some relevant examples which deserve to be mentioned in this report.

A first series of games are role-playing games in which players assume a fictional role, often that of organisations who collect and deal with personal data. The scope of these role-playing games is to make players understand how their personal data are collected, managed and used, often by very ruthless organisations. A first example is the game *Data Dealer*[95] a non-profit project and licensed under Creative Commons in which "*players take on the role of unscrupulous "data dealers", collect personal data all over the internet, and learn how to turn this information into cash*"[96]. Data Dealer is a browser game that promotes awareness about how companies could collect personal data and the use they can make of this data, and this is achieved by offering player the opportunity to take the role of these companies and collect and exploit personal data. The game has received relevant news coverage and won the *Most Significant Impact* Games for Change award in 2013[97].

[95] See http://datadealer.com
[96] See http://datadealer.com/about
[97] See http://www.gamesforchange.org/2013/06/winners-of-the-g4c-awards-announced/



Graph 2 – Screenshot of the Data Dealer educational game[98]

A non-digital game with a similar approach, was the *Privacy Traders*, a role-playing game originally developed for the Internet Governance Forum Italy in 2011. The game was aimed at high school students to be played in class. In this role-play game, students playing in groups could take the role of four or more social networks and the scope of the game is to collect personal information of participants. The winner will be who has collected the larger amount of personal data of other participants. In this way students would learn that the key business practice of Social Network Sites is indeed the collection and exploitation of personal data and that a Social Network account does not just come "for free" as users in fact trade in their personal data. An interesting aspect of the *Privacy Traders* was that its content and gaming outcomes were clearly linked with the work of the Italian Privacy Authority (so-called *Garante Della Privacy*), as the game was accompanied by the explanation from an expert[99] of how Privacy regulations in Italy would apply to collection of personal data. Young people participating to the game received then also notions about privacy regulations in Italy and how companies collecting private data should behave in accordance to regulation. Similar to the previous two examples is the *Privacy Game* proposed by the Open University[100], again a role-playing game in which players assume the role of a fictional character and "*make decisions about what information characters might reveal to others and what they keep to themselves*". In this case the role assumed is not that of a company collecting data, but that of a data subject (e.g. Internet Shopper, Employer or even Hacker). The learning goal of the game is to highlight for players the value of personal information as commodity. Another interesting example was the game *Friend Inspector*[101]. While the above discussed role-playing games are general purpose in their application, Friend Inspector was a game directly aimed at Facebook users and it had an explicit goal: raising awareness of Privacy in Social Network Sites. Friend Inspector was a browser game that allowed participants to check who can see their Facebook account and what information they have access to. The game also offered final

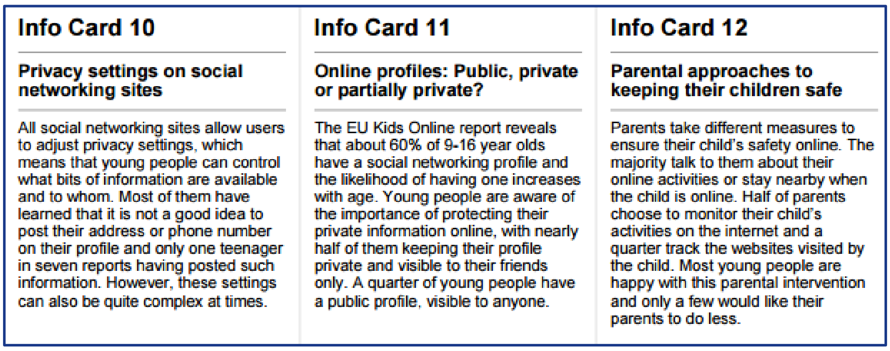
[98] The game, including this image is released with a Creative Commons license Attribution-ShareAlike 3.0 (CC-BY-SA 3.0)

[99] The expert presentation (in Italian) is also available as a Youtube video as part of the "game pack", see https://www.youtube.com/watch?v=9irSEkdQDfs

[100] The game is hosted by the Centre for Research into Information, Surveillance and Privacy (CRISP)

[101] See http://www.friend-inspector.org/

recommendations on how players can improve their privacy on Facebook[102]. The game is now inactive due to Facebook change of privacy policy as the end of April 2015. An additional example is a game created by the Pan-EU Youth project[103] using the game format play-decide[104]. These games offer young people the opportunity to "*Organise vivid debates with your friends at home or in the classroom and come up with a policy on different issues on online responsibility and digital literacy*"[105]. Specifically, the Privacy and Data Protection play-decide game[106], is a card game in which young people have the opportunity to debate issues surrounding Privacy and is organised in three stages[107], according to the play-decide format. The first stage is the initial gathering of information supported by a set of cards containing information about Privacy and Data Protection facts. The second step is a group discussion in which participants talk about key themes of Privacy and Data Protection, again using a set of cards. The third and final stage is the outcome of the game in which participants reach the formulation of policies on Privacy and Data Protection. An interesting aspect of the game is that the policies formulated by playing the game can later be shared on the Pan-EU Youth website. A last example of a game in the European Context is the "The earthquake data"[108] a card game for 2-4 people, which has been created for students of secondary schools and vulnerable adults. The game is only available in Polish language under the original name of "Trzęsienie danych" and has been created by the Panoptykon Foundation[109]. The game offers information to players on how to better protect their privacy in everyday life. The game cards contain links to articles on the web with additional information and practical advice.



Info Card 10	Info Card 11	Info Card 12
Privacy settings on social networking sites	**Online profiles: Public, private or partially private?**	**Parental approaches to keeping their children safe**
All social networking sites allow users to adjust privacy settings, which means that young people can control what bits of information are available and to whom. Most of them have learned that it is not a good idea to post their address or phone number on their profile and only one teenager in seven reports having posted such information. However, these settings can also be quite complex at times.	The EU Kids Online report reveals that about 60% of 9-16 year olds have a social networking profile and the likelihood of having one increases with age. Young people are aware of the importance of protecting their private information online, with nearly half of them keeping their profile private and visible to their friends only. A quarter of young people have a public profile, visible to anyone.	Parents take different measures to ensure their child's safety online. The majority talk to them about their online activities or stay nearby when the child is online. Half of parents choose to monitor their child's activities on the internet and a quarter track the websites visited by the child. Most young people are happy with this parental intervention and only a few would like their parents to do less.

Graph 3 – Examples of Information Cards from the "play-decide game on Privacy and Data Protection"

[102] See for a publication on Friend Inspector: Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., Sänger, J., "Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks", In Proc. of the 2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion (IDGEI), 2014

[103] http://paneuyouth.eu/

[104] The play-decide format has been developed by FUND project funded by the European Commission, see http://www.playdecide.eu/play/howto

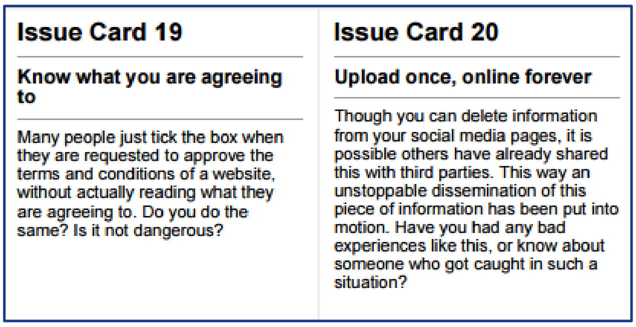
[105] See http://paneuyouth.eu/playdecide/

[106] See http://paneuyouth.eu/files/2012/09/PD-kit-privacy-and-data-protection-2.pdf

[107] The play-decide game on Privacy and Data Protection is released under the Attribution Share-Alike 3.0 Unported License.

[108] See http://cyfrowa-wyprawka.org/teksty/zagraj-w-trzesienie-danych - the game is distributed under a Creative Commons License BY-SA 3.0 GB

[109] See https://panoptykon.org/about-panoptykon



Issue Card 19

Know what you are agreeing to

Many people just tick the box when they are requested to approve the terms and conditions of a website, without actually reading what they are agreeing to. Do you do the same? Is it not dangerous?

Issue Card 20

Upload once, online forever

Though you can delete information from your social media pages, it is possible others have already shared this with third parties. This way an unstoppable dissemination of this piece of information has been put into motion. Have you had any bad experiences like this, or know about someone who got caught in such a situation?

Graph 4 – Examples of Issue Cards from the “play-decide game on Privacy and Data Protection”

Two additional examples outside the European context deserve to be mentioned here, as they present some relevant differences from the examples cited before. The first is a game developed by the Canada’s Centre for Digital and Media literacy, called *Privacy Playground: The First Adventure of the Three CyberPigs*[110]. As stated on the teacher’s guide *“The purpose of the game is to teach kids how to spot online marketing strategies, protect their personal information and avoid online predators*[111]*”*. Of particular interest is that the game cater for a very young audience of pupils between 8-10 years of age. The game is a graphical novel which readapts the story of the three little pigs and guides players trough scenarios and quiz related with Privacy and the protection of their personal data. The second game is called *Privacy and Security Challenge*[112] and was created by The Office of the National Coordinator for Health Information Technology's (ONC) Office of the Chief Privacy Officer (OCPO) in the United States. This example is different from the others discussed so-far as the game is used for training in first response situations, i.e. situations that are dangerous or difficult to conduct in reality. Specifically the game aims at training health care provider professionals (e.g. nurses) to respond to Privacy and security challenges faced in a typical small medical practice. This is a relevant approach leveraging serious games for training that clearly go beyond raising awareness only. This is the only example identified in this short review that leverages this approach to training professionals.

In conclusion, serious games are a path which is being explored as a way to transfer knowledge, support learning, raise awareness, offer professional training and unveil controversial issues and practices surrounding Privacy and Data Protection. There are some relevant points to consider in conclusion of this section. The landscape of serious gaming appear quite fragmented and some of the existing games, while interesting, do seem now abandoned (e.g. Privacy Traders) or obsolete due to various reasons (e.g. Friend Inspector, due to Facebook change of Privacy Policy). Of relevance of the gamified approach is the use of gaming to reach a varied audience from very young people (e.g. pupils, high school students), to citizens, to professionals. This shows how gamified approaches are flexible tools for dissemination, learning and awareness at different levels and the recommendation is to continue exploring serious gaming in the area of Privacy and Data Protection. Another interesting aspect to consider is that a good number of the games discussed here is released under Creative Commons licenses[113], this is a best practice that can support wider re-play and in some cases further adaptations of the games. In particular non-digital games often come with downloadable game “packs”, so that interest parties (e.g. schools) can download the game material and instructions and print it for their own play. It is also relevant to note that there is interest in

[110] See http://mediasmarts.ca/game/privacy-playground-first-adventure-three-cyberpigs
[111] See http://mediasmarts.ca/sites/mediasmarts/files/pdfs/games/privacy_playground_guide_2015.pdf
[112] See http://www.healthit.gov/providers-professionals/privacy-security-training-games
[113] See http://creativecommons.org/

developing serious games that are non-digital/offline (e.g. board, card games) that can be played collectively and in person by participants. This is an important best practice. Indeed, digital games (including quizzes) are often single-player[114] and therefore less able to support peer-learning and critical discussion among players and between players and facilitators (e.g. teachers). Finally a further possible recommendations is that games should also be accompanied by processes of evaluation of their results. This would be relevant in order to verify how effective the gamified approach is for learning or training and what could be done better in Privacy and Data Protection Games.

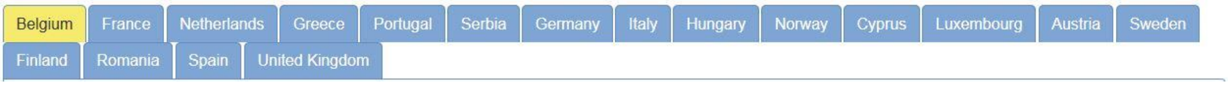
[114] To this is an exception Open University *Privacy Game* that supports both single and multiplayer games.

5. Educational tools

5.1 The new version of the Education map[115]

A database has been created by ENISA with information on Network and Information Security courses in Europe in the context of a close partnership with WG3 of NIS Platform. It was launched in October 2014 with the context of the advocacy campaign European Cyber Security Month. The database lists a number of available courses and certification programmes linked to Network and Information Security, privacy and data protection.

ENISA is working to enhance the database and the 2015 version contains relevant improvements among which it is important to mention: improvements to the search functionality, a better display of the information which will ease users in consulting the available material and finally a better promotion of the database towards education providers that will facilitate and support them to encode and add their offers to the database. Regarding metrics and current size of this tool: after +1 year of existence this map displays 22 countries in Europe and includes more than 400 entries. ENISA encourages Higher Education and Long Life Learning providers to include their offer in this map.



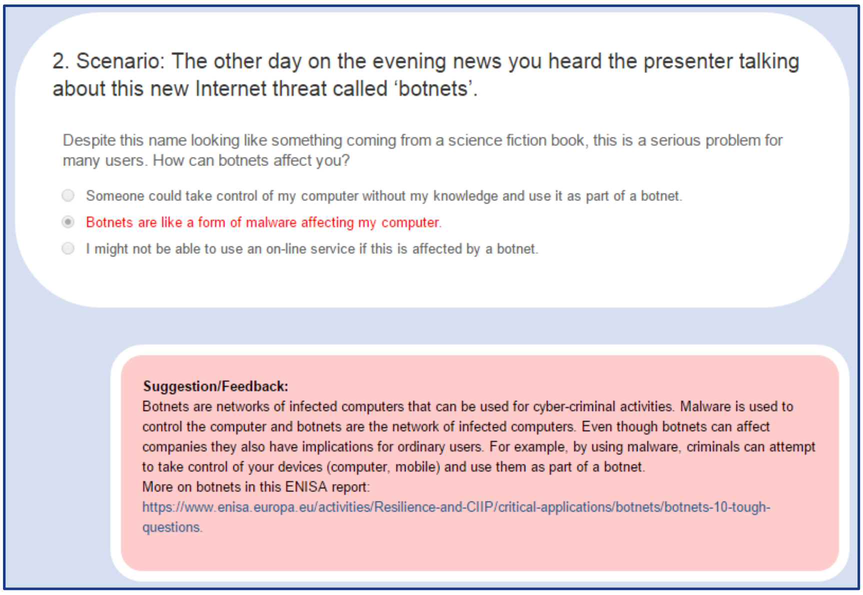
Graph 5- existing entries on the map year 1

5.2 The NIS quiz from pilot to version 1.0

In 2014, as part of the European Cyber Security Month[116] and its NIS eEducation activities, ENISA has developed a NIS self-assessment pilot quiz. The pilot quiz has originally been created with several goals in mind. The first one is to disseminate best practices and notions around NIS – with particular emphasis on general security and privacy - to a broad non-specialist audience. The model of the questions chosen for the quiz has been that of a scenario, in which a narrative-short story is presented to participants and then three options are offered as possible answers to the scenario problem. Participants are then asked to select one of the options. Upon selection of an answer – whether correct or not – an explanation/feedback is offered to participants on why the answer is correct or not within the context of the scenario. In addition to the textual feedback, additional links to relevant material to consult are also offered. In this way participants can with a single click, access relevant report and additional content. In graph 6 there is an example of a question taken from the 2014 pilot quiz: a scenario is presented to participants – in the example in graph 6 a scenario about botnets – then three options/answers are presented.

[115] See https://cybersecuritymonth.eu/references/universities
[116] See https://cybersecuritymonth.eu/

In the example the participant has selected an incorrect answer and then there is the explanation/feedback about the answer with a pointer to an ENISA report for more information.



2. Scenario: The other day on the evening news you heard the presenter talking about this new Internet threat called 'botnets'.

Despite this name looking like something coming from a science fiction book, this is a serious problem for many users. How can botnets affect you?

○ Someone could take control of my computer without my knowledge and use it as part of a botnet.

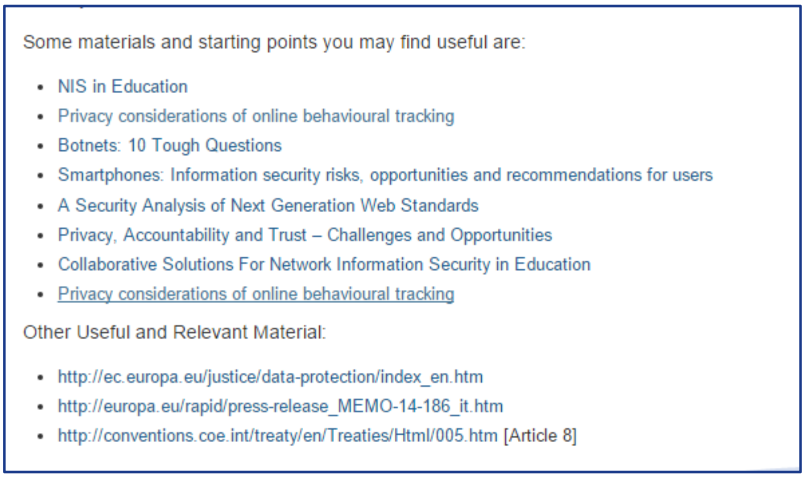
● Botnets are like a form of malware affecting my computer.

○ I might not be able to use an on-line service if this is affected by a botnet.

Suggestion/Feedback:
Botnets are networks of infected computers that can be used for cyber-criminal activities. Malware is used to control the computer and botnets are the network of infected computers. Even though botnets can affect companies they also have implications for ordinary users. For example, by using malware, criminals can attempt to take control of your devices (computer, mobile) and use them as part of a botnet.
More on botnets in this ENISA report:
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-10-tough-questions.

Graph 6 – Example of a scenario and the feedback on an incorrect answer from the pilot quiz.

A second goal of the quiz was to combine together an entertaining-gamified activity with a serious educational goal: offer via a quiz-game an opportunity for participants to familiarise themselves with some of the key themes of NIS Education and some of the recommendations contained in a number of ENISA reports. In this way the quiz also served a third goal: better disseminate part of the ENISA work to citizens and other interested stakeholders. In particular several questions of the pilot quiz have been created using a number of ENISA reports and recommendations – mainly those aimed at end users – and references to reports are offered in the feedback to each answer. In addition, at the end of the quiz a list of all the reports used for building the quiz is presented to participants (see graph 7).



Some materials and starting points you may find useful are:

- NIS in Education
- Privacy considerations of online behavioural tracking
- Botnets: 10 Tough Questions
- Smartphones: Information security risks, opportunities and recommendations for users
- A Security Analysis of Next Generation Web Standards
- Privacy, Accountability and Trust – Challenges and Opportunities
- Collaborative Solutions For Network Information Security in Education
- Privacy considerations of online behavioural tracking

Other Useful and Relevant Material:

- http://ec.europa.eu/justice/data-protection/index_en.htm
- http://europa.eu/rapid/press-release_MEMO-14-186_it.htm
- http://conventions.coe.int/treaty/en/Treaties/Html/005.htm [Article 8]

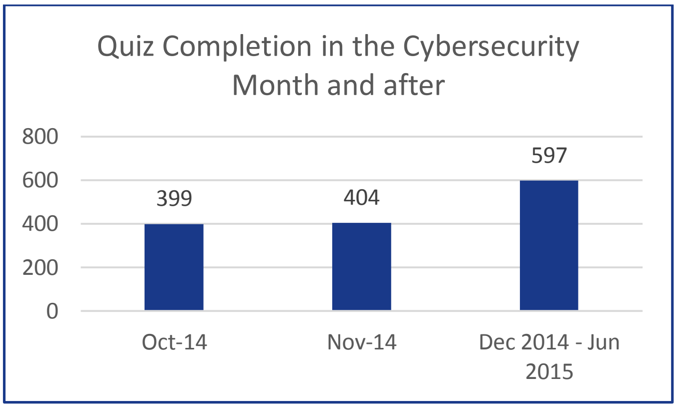
Graph 7 – List of ENISA report presented at the end of the quiz to participants on which the pilot quiz is based

The pilot quiz has received positive feedback from citizens, experts and public authorities. Most importantly the quiz was completed by a good number of participants (see data in the next paragraph) across the world. Therefore building on the encouraging results of the pilot, this year ENISA has continued working on the idea of a quiz as an important approach to disseminate NIS practices to a wider audience of non-experts. The approach adopted for the 2015 edition of the quiz, considers: overcoming shortcomings observed in the test-pilot as well, make improvements in the areas of content and usability and keep intact aspects of the pilot that worked well in particular the format of the question and the dissemination of ENISA material. Therefore the goal for this year work is to make the pilot evolve into a more stable and solid quiz, with additional questions, better scenarios, graphical and general use improvements. In the following paragraphs some reflections are offered on the results of last year work and there is a presentation of key results from last edition of the quiz. There is also a discussion about how these results have informed the new quiz this year. There is then a discussion of the key aspects of the new version of the quiz.

5.2.1 Results achieved with the pilot quiz in 2014

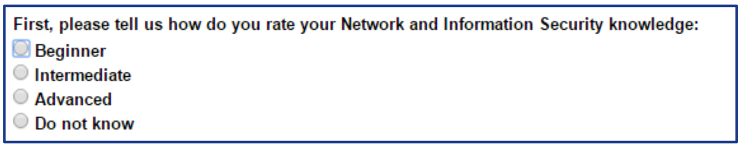
In this section of the report are present some data and results of the 2014 pilot quiz. Both numerical data related with participation and examples of the textual feedback received from participants are presented. These data have been taken in account to inform decisions for this year work on the quiz.

The pilot version of the quiz was launched by ENISA as part of the European Cyber Security Month activities on 23 October 2014. In term of overall participation the quiz page has been visited by almost 40.000 (thousands) users and the quiz was completed (from start to finish) by 1400 participants. The quiz has also been completed by participants from 81 countries, with clear prevalence of EU countries – with some exceptions (United States and India also appear in the list of top 10 countries, perhaps due to the quiz being in English). In the top 10 list of countries we have Belgium, United Kingdom, Greece, Netherlands, Italy, Germany, Spain and Estonia. While the number of participants that completed the quiz and the spread across the globe are very encouraging, there is also a gap between the number of unique visitors to the quiz (almost 40 thousands) and the number of those who completed it. This is an aspect which will be taken in account this year and improvements are planned to increase the number of people completing the quiz from start to finish. In graph 8 is displayed the breakdown of participation across the period of the Cyber Security Month (October – November) and the remaining months up to June 2015, when the work on the new version of the quiz started.



Graph 8- Monthly breakdown of participants – with emphasis on the Cybersecurity Month period.

During last year piloting work, particular emphasis was placed on offering participants the opportunity to give impressions, comments and feedback to ENISA. The goal was to collect material that could be used for making improvements for future editions of the quiz and also listen to participant ideas. An important aspect of this was the initial self-assessment of participants. ENISA together with its experts agreed that the quiz should be a simple way to measure some of the participants' skills related to NIS but should also offer a way for participants to identify knowledge and skills gaps and offer information on how to bridge these gaps. The quiz came with diverse levels of difficulties and at the beginning participants were asked to self-assess their level of knowledge, according to three different levels - beginner, intermediate, advanced and do not know[117] - and where, upon their selection, thus directed to the appropriate level quiz.

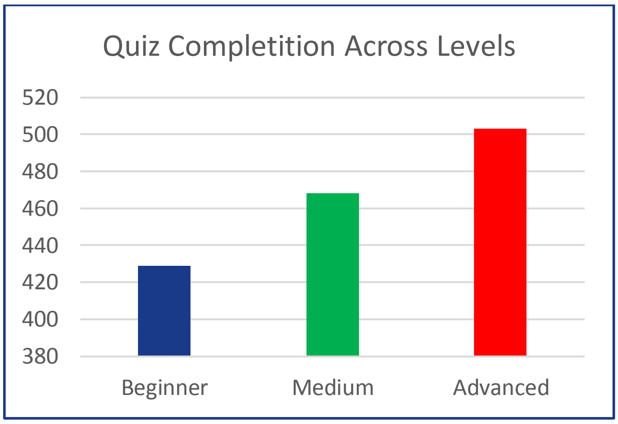

First, please tell us how do you rate your Network and Information Security knowledge:
○ Beginner
○ Intermediate
○ Advanced
○ Do not know

Graph 9 – Form of the Preliminary self-assessment for participants

In graph 10 it is possible to see the breakdown of participants in terms their initial self-assessment. The quiz has been completed most at the advanced level (503 completion) and less at the beginner level (429 completion) although the variation between the two is not enormous. In perspective this tells probably that more work needs to be done to increase participation and engagement for non-expert, as they were indeed the main target audience for the 2014 pilot quiz. For this year edition the key focus will indeed be

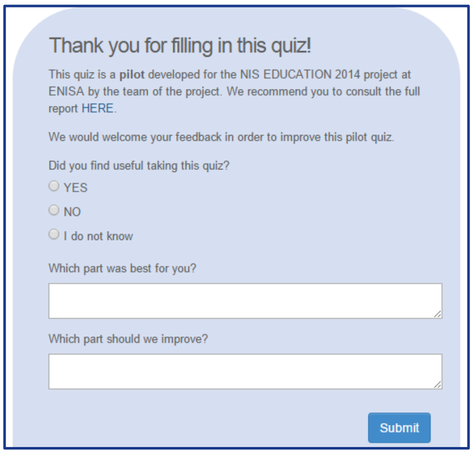
[117] The selection of the "do not know" option would lead participants to the beginner version of the quiz.

on the beginner and intermediate levels of the quiz. A further consideration made during the discussion of the experts is that probably the label "beginner" is not the most appropriate as it might point to weaknesses of participants and for this year this will be replaced with more neutral labels (e.g. "initial level" or "level 1"). An additional feature of the pilot quiz was also that upon good results in a lower level of the quiz (e.g. beginner) the platform would encourage participants to take the next advanced level (e.g. intermediate), thus encouraging participants to learn more and have a better sense of their knowledge. This feature could also have had some impact on the increase rate in completion leaning toward higher levels, however analytics measures for this aspect are not available.



Graph 10 - Breakdown of participants based on their self-assessment

In addition to the self-assessment, the pilot quiz did offer participants opportunities to provide textual feedback to ENISA, both in term of their expectations about the quiz (prior to start the quiz) and at the end as a general feedback about the engagement with the quiz asking what could be improved and what they enjoyed about the quiz. The purpose for asking participants their comments was to gather evidences about the relevance of this initiative directly from participants and have material to be used for shaping and improving future editions of the quiz. In graph 11 is presented the feedback from appearing at the end of the pilot quiz.



Thank you for filling in this quiz!

This quiz is a **pilot** developed for the NIS EDUCATION 2014 project at ENISA by the team of the project. We recommend you to consult the full report HERE.

We would welcome your feedback in order to improve this pilot quiz.

Did you find useful taking this quiz?

○ YES
○ NO
○ I do not know

Which part was best for you?

Which part should we improve?

Graph 11- Feedback form at the end of the 2014 pilot quiz

Hereafter are presented some examples of the feedback received from participants and this is followed by a discussion about how the key feedbacks have informed the new version of the quiz. Some examples of what the participants did like about the quiz:

It was reassuring and the responses after each question explained the answers simply.

I have learnt a little bit more about security. Now I assess the links that will help me to improve my knowledge about security in the internet.

On the questions that I got wrong, the correct answer had good feedback with i.e. links to articles that explain it all in (more) detail.

These comments point to relevant strengths of the quiz, in particular the opportunity for participants to learn more about security and the emphasis placed on detailed feedback and additional material to consult. As already discussed, these elements will remain part of the new version of the quiz.

The following are suggestions about what could be improved and done better:

I think some of the questions were a bit ambiguous - it is difficult from the description to pick one particularly correct answer when more than one of the actions may be reasonable. Appreciate this is difficult to get right with this sort of quiz.

Some of the answers should be explained a little bit more as to understand the right idea behind them.

Language, I think the different scenarios could be described in a simpler language, therefor enabling easier access to the non-native English speakers.

These feedback points to some of the weaknesses of the quiz, and in particular the wording of scenarios and answers which on occasion could be simplified hence offering a better understanding to participants. Also these considerations have been taken in account for this year work.

5.2.2 Usability and other issues in the pilot version

The pilot version of the quiz has been reviewed both by usability experts and by the experts collaborating with ENISA in term of its usability and graphical appealing and several improvements have been discussed and planned for the new version in 2015, also taking in account the users' feedback. Recommendations output of this review include:

- The introduction of multimedia material (rather than having just a textual quiz) where possible, in order to: improve the general and lasting engagement with the quiz, offer better explanations to participants, support participants across the whole breadth of the quiz and increase the number of full completion of the quiz.

- Better explanation of why a certain answer is correct within a scenario. Since the questions are based on a narrative, answers are contextual to the narrative itself. One of the recommendations received relates with the idea of offering better explanations as to why a specific answer is indeed correct in the scenario, and not necessarily in general.

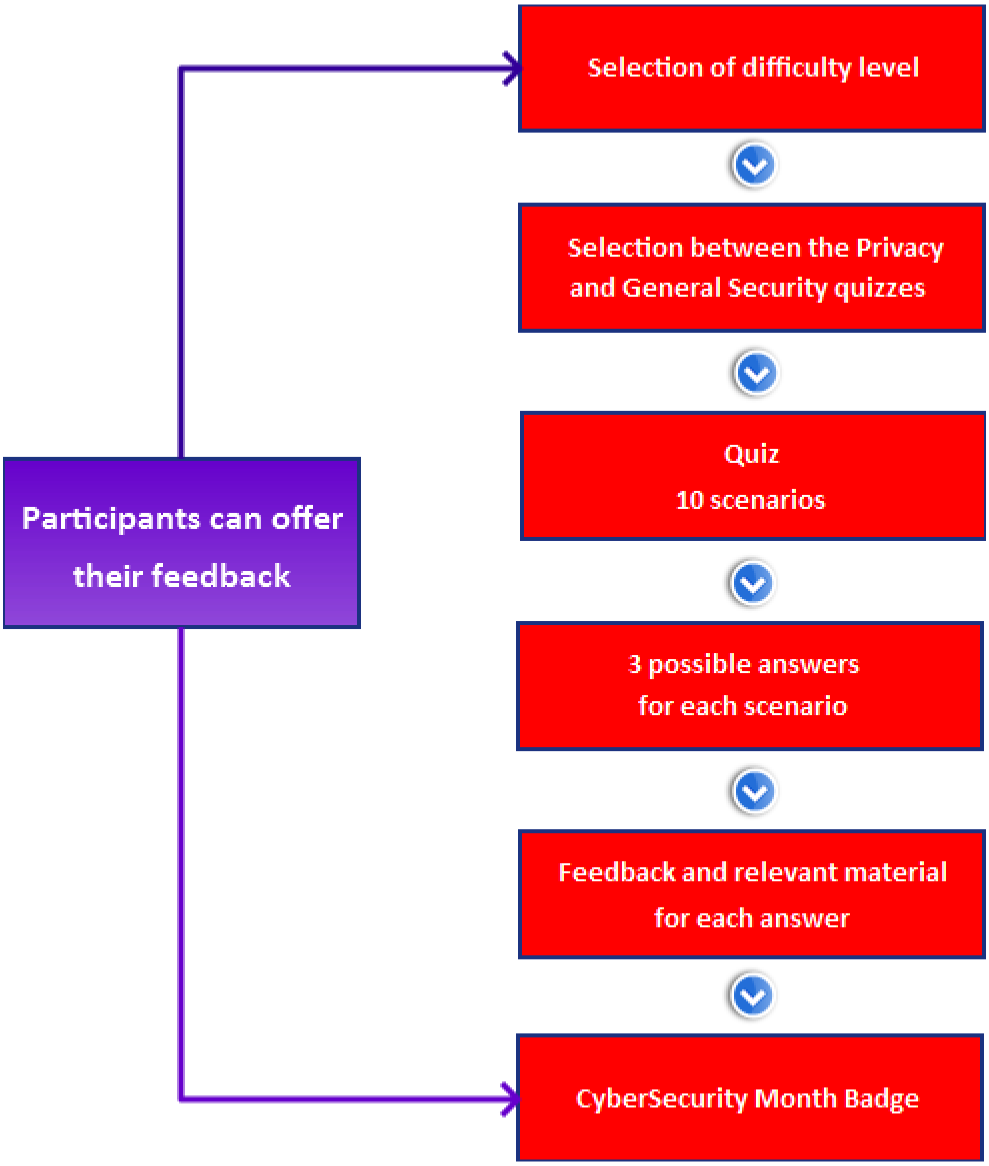
- Increased number of quizzes. The pilot version was developed as a single quiz covering several NIS areas. A relevant addition, already discussed also during the work of the experts both in 2014 and 2015 is to have quizzes organised around different topics (e.g. privacy or security etc.). Hence to have multiple quizzes with participants being able to take them individually but also together for instance with the award of the badge based on aggregated scores from the diverse quizzes.

- To improve the gamification elements of the quiz. In the pilot version, these were limited to the generation of a profile and score at the end of the quiz. A relevant addition to this year quiz are Cyber Security Month badges that are awarded upon completion of the quiz and that participant can share on Social Media. The use of badges is also one of the measures adopted for supporting the full completion of the quiz by a larger number of participants.

Generally the idea is to: offer better textual descriptions, streamline the number of quizzes across diverse subjects, improve the gamification aspects to create better engagement and add multimedia material to better support the completion of the quizzes by participants. In the next section there is a discussion of how these recommendations have shaped the new version of the quiz.

5.2.3 Version 1.0 of the Quiz

The general concepts and organisation of the 2015 quiz will remain similar to the original 2014 pilot (see Graph 12). With some relevant improvements that are briefly presented in this section. The participant will choose the difficulty level then select the choice between topics: Privacy or General security. Furthermore they will reply to 10 scenarios by choosing an answer from the provided ones. Each answer will come with an explanation and at the end a Cyber Security Month badge.


Selection of difficulty level
Selection between the Privacy and General Security quizzes
Quiz 10 scenarios
3 possible answers for each scenario
Feedback and relevant material for each answer
CyberSecurity Month Badge
Participants can offer their feedback

Graph 12 – Structure of the 2015 quiz

The questions will be presented to participants as scenarios/narratives with 3 options/answers among which to choose. Similarly to the 2014 edition each answer will be accompanied with specific feedback and additional material to consult. This approach has indeed proven successful for disseminating best practices and for driving engagement. The feedbacks received from participants about this format have also been encouraging. Relevant changes introduced this year in comparison to last year pilot are the following:

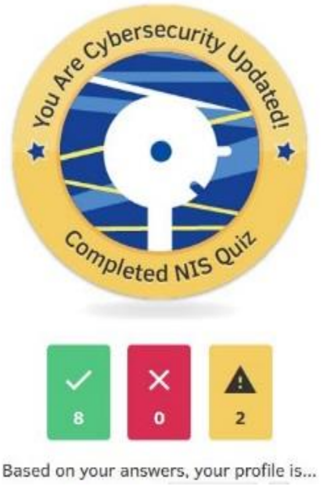
- For this year there will be two quizzes rather than just one: one quiz will be devoted to general security and the other one to privacy. This will be achieved by splitting the 2014 pilot quiz questions (i.e. dividing those related with privacy from those related with security) and adding additional questions to sum up to 10 questions for each quiz. In this way last year work will be capitalised and extended, offering more content alongside the content already produced.

- In this edition there will be two difficulties levels for the quiz, those that in the early pilot corresponded to beginner and intermediate levels. The reason for this choice is the will to engage with the quiz mainly the general audience rather than security experts, hence more effort is devoted to develop a quiz for this specific audience which is the one that could receive additional benefits from the quiz.

- The Usability of the quiz has been substantially improved with: (1) a virtual avatar acting as a “guru guide” through the quiz, in order to make the quiz more personal and increase the engagement, (1) one short explanatory video in order to increase engagement and offer better explanations of the goals and achievements of the quiz.

- Wording of 2014 scenarios, answers and feedbacks has been simplified were possible. For new questions developed in 2015 wording has been kept simpler in comparison to 2014 questions. In this way the key feedback received from users will be addressed.

- The version 1.0 will use a better gamified approach. Among other things this year there has been the introduction of Cyber Security Month Badges, in order to offer a better engagement, reward and opportunity to share results on Social Media.



Based on your answers, your profile is...

Graph 13- Mock up figure of our badges!

6. Conclusion

This report has provided an initial mapping and a discussion about existing education and training opportunities with particular focus on ePrivacy and has connected these with the wider offer of NIS education discussed in the previous 2014 report *Roadmap for NIS education programmes in Europe*. What has emerged from this analysis are strengths and weaknesses in the current landscape, but most importantly several relevant best practices have been identified and possible improvements have been signalled. What follows is a list of initial recommendations (both at EU and MS' levels) based on the results of the report, EU level organisations (e.g. University Networks, Users' Coalitions and Multipliers, Education institutions); Member State level organisations (e.g. Education institutions, NGOs, think tanks, Governments).

6.1 For European level stakeholders

- Consider to analyse the quantity of the offer of courses in MSs.
- Consider to conduct further research to better understand how Privacy subjects are embedded in undergraduate degrees. The report has highlighted that Privacy does not seem to feature in titles of undergraduate degree courses and further research would be required to understand why (e.g. if it is for marketing purposes or if there is a skill gap in current offer).
- Consider to invest in MOOCs on Privacy and Data Protection, covering both basic and advanced topics, for non-expert and expert audiences. There is a general lack of Privacy and Data Protection MOOCs in the EU context, however this delivery opportunity could be better exploited also via existing supported platforms (i.e. OpenUpEd and EMMA).
- Consider to invest in MOOCs with a NIS focus, in particular addressing the issue of privacy-by-design and European Legislation. The report has highlighted that there is scope for some specific MOOCs relating with issues currently debated at a European Level.
- Consider to further explore serious games as a path to reach a varied audience of both experts and non-experts. In particular, serious games should support re-playability and ideally be distributed with non-restrictive licenses in order to support adaptation and wider reuse in educational settings and by the public more generally. Consider investing resources also on the evaluation of results achieved with serious games.
- Consider exploring serious gaming not only for raising awareness but also as a training ground for first-responders and other professionals. In the European context, serious games around Privacy and Data Protection focuses extensively on education and awareness. While these are fundamental aspects, there is also scope for using serious games for training first response professionals.

6.2 For Member State level

- Consider to create synergies with other countries in terms of transfer of best practices.
- Consider to create metrics and assess the progress and the offer from the education providers.
- Games available in one of the MS language could be translated to other languages, for a wider impact, when applicable. The use of Creative Commons licenses could support this.
- The report has highlighted that some of the existing MOOC are available in National Languages, this is clearly an advantage and a good practice. Other MSs could consider develop Privacy and Data Protection MOOCs in the respective MS' languages.
- Should consider to explore the offer of serious games and enrich it.
- Consider to join ENISA's project quiz in order to raise awareness by participating in the spread of general quizzes and awareness month.

Annex A: References and tables

Websites, visited during the period July- October 2015

- E-Privacy Directive http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
- ENISA Education report http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe
- Eskills website http://eskills-vision.eu/about/e-skills-gap/
- ENISA report smart homes https://www.enisa.europa.eu/media/press-releases/are-smart-homes-cyber-security-smart
- European Cyber Security Month website www.cybersecuritymonth.eu
- ENISA report privacy by design http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design
- Digital agenda website http://ec.europa.eu/DocsRoom/documents/7146
- Information Commissioners Office - Data protection rights: What the public want and what the public want from Data Protection Authorities (2015) https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf
- EDPS website https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Legislation
- EFF website https://www.eff.org/about
- Privacy International website https://privacyinternational.org/?q=reports
- AIPCA website http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/InternationalPrivacyConcepts.aspx
- BakerHostetler website http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf
- DLA Piper Data Protection Laws of the World Handbook http://dlapiperdataprotection.com/#handbook/ and map http://dlapiperdataprotection.com/#handbook/world-map-section
- OCR. (2011) GCSE in Computing J275 at http://www.ocr.org.uk/images/81949-specification.pdf
- AQA. (2015) GCE AS and A Level Specification Computing at http://filestore.aqa.org.uk/subjects/specifications/alevel/AQA-2510-W-SP-14.PDF
- UCAS website https://www.ucas.com/

- Prospects search http://www.prospects.ac.uk/search_courses_results.htm?t=srs&criteria.keyword=privacy&addfilter=2022
- IAPP Privacy Association website https://privacyassociation.org/
- European Commission http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf
- ECDL website www.ecdl.org
- ICS- skills website http://www.ics-skills.ie/data-protection/essentials.php
- AICA website http://www.aicanet.it/aica/diritto-ict
- BCS website http://www.bcs.org/category/5651
- Data Protection Commissioner IE http://www.dataprotection.ie/docs/Training-and-Awareness/805.htm
- PRIPARE project http://pripareproject.eu/events/privacy-training-workshop-3/
- STARTIFY project http://www.startify7.eu/trento
- EDTECH Magazine http://www.edtechmagazine.com/higher/article/2014/02/harvardxs-and-mitxs-mooc-data-visualized-and-mapped
- EdX platform www.edx.org
- Openuped platform www.openuped.eu
- European MOOCS platform www.platform.europeanmoocs.eu
- Miriadax platform https://www.miriadax.net/web/derecho-redes-sociales
- MOOC list website https://www.mooc-list.com/
- FUN MOOC https://www.france-universite-numerique-mooc.fr/about
- Info Secure website http://www.infosecuregroup.com/CSI.html
- Vermont INFOSEC website http://itsecurity.vermont.gov/Fun_with_Security/games
- Carnegie cyber academy http://www.carnegiecyberacademy.com/funstuff.html
- Quiz http://newsquiz.sciencemag.org/privacy/
- Quiz on UK Information Commissioner Office https://ico.org.uk/about-the-ico/privacy-and-data-protection-quiz/
- Daten Schutz quiz https://datenschutzquiz.hs-kl.de/
- Verbrauchercentrale website http://www.verbraucherzentrale-rlp.de/datenschutz-quiz
- Office of Privacy Commissioner of Canada quiz https://www.priv.gc.ca/youth-jeunes/quiz/index_e.asp
- Klicksafe quiz http://www.klicksafe.de/qz/quiz03/_project/

- Data Dealer website http://datadealer.com/about
- Games for change website http://www.gamesforchange.org/2013/06/winners-of-the-g4c-awards-announced/
- Game Friend Inspector http://www.friend-inspector.org/
- Panyouth website http://paneuyouth.eu/
- FUND project game http://www.playdecide.eu/play/howto
- Cyfrowa game http://cyfrowa-wyprawka.org/teksty/zagraj-w-trzesienie-danych
- Panoptykon Foundation website https://panoptykon.org/about-panoptykon
- Media Smart http://mediasmarts.ca/game/privacy-playground-first-adventure-three-cyberpigs
- Health It games http://www.healthit.gov/providers-professionals/privacy-security-training-games
- Creative Commons website http://creativecommons.org/

Articles and publications

- Touraine, A. (1988). Return of the Actor Social Theory in Postindustrial Society. Minneapolis: University of Minnesota Press.
- Bell, D. (1976, May). The coming of the post-industrial society. In The Educational Forum (Vol. 40, No. 4, pp. 574-579).
- Castells, M. (2000). The information age: economy, society and culture. Vol. 1, The rise of the network society (Vol. 1). Oxford: Blackwell.
- Fuchs, C. (2007). Internet and society: Social theory in the information age. Routledge.
- Clarke, R. (2006, July). What's privacy? Available here: http://www.rogerclarke.com/DV/Privacy.html
- Buchmann, J. (2014). Internet Privacy: Options for adequate realisation. Springer Science & Business Media.
- Colvin, K., Champaign, J., Liu, A., Zhou, Q., Fredericks, C., & Pritchard, D. (2014). Learning in an introductory physics MOOC: All cohorts learn equally, including an on-campus class. The International Review Of Research In Open And Distance Learning, 15(4). Retrieved fromhttp://www.irrodl.org/index.php/irrodl/article/view/1902/3058
- Susi, T., Johannesson, M. & Backlund, P. (2007). Serious games – An overview, (Technical Report HS-IKI-TR-07-001). Retrieved from http://www.his.se/PageFiles/10481/HS-IKI-TR-07-001.pdf
- Article on the Computer World Magazine about using gamified approaches to training in security http://www.computerworld.com/article/2489977/security0/boost-your-security-training-with-gamification-really.html .

- Blog post from SANS on the gamification of security awareness http://www.securingthehuman.org/blog/2012/01/17/gamifying-security-awareness .
- Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., Sänger, J., "Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks", In Proc. of the 2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion (IDGEI), 2014
- Article on WSJ http://www.wsj.com/articles/how-much-do-you-know-about-data-privacy-1429499471.
- Article on Ilsole24ore http://www.ilsole24ore.com/art/tecnologie/2014-01-29/conosci-privacy-web-072247.shtml?sondaggi .
- Article on http://www.journaldunet.com/questionnaire/fiche/14520/d/f/1/ .

Table and graphs list

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number TP-01-15-592-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-127-4
DOI: 10.2824/402788