enisa

European Network
and Information
Security Agency

Collaborative Solutions For Network Information Security in Education

About ENISA

The European Network and Information Security Agency (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

Follow us on Facebook Twitter LinkedIn YouTube & RSS feeds

Contact details

For contacting ENISA or for general enquiries on **EDUCATION** refer to Daria CĂTĂLUI, editor of this report, using the following details:

- E-mail: awareness@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Acknowledgements

The ENISA team would like to thank the experts who took the survey and participated in the online sessions to gather information for this report. Our gratitude also goes to Prof. Dr. Ingrid Schaumüller-Bichl from Austria, Albin Wallinger and the team from Luxembourg, authors Pernille Tranberg and Steffan Heuer for their collaboration and contributions to the report.

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 an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of the-art and it might be updated 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. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. 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. Reproduction is authorised provided the source is acknowledged.

Contents

1 Executive Summary

This report, ‘Collaborative Solutions For Network Information Security in Education’, is a **continuation of the work undertaken in 2011** which resulted in the publication of the report ‘Network Information Security in Education: Consolidated ENISA contribution’.[1]

This report explores ways in which educators can get full use out of information technologies while promoting and providing education on the importance of network information security.

We argue that brokerage of information is the basis of the learning cycle and we provide details to justify this by using practical examples. **The main recommendation arising out of this work is that we should all learn from best practices of our peers and share our own experience**. We also recommend that a **‘can do’ attitude’** should be deployed by educators and their students of different age groups.

This report is aimed at educators, defined as trainers, teachers, peers involved in formal education and non-formal education, including lifelong learning.

The report consists of three parts, each of which is equally important, namely **the results of the survey and consultations**, the **ENISA recommendations** from 2012 deliverables and **three case studies from Member States (Austria, Luxembourg and Denmark)**. As Commissioner Nellie Kroes stated when referring to digital tools, it is important to realise the huge benefit for economies, societies and democracies that are brought by such digital tools and to participate in the effort to ‘build a connected, competitive continent: an e-EU’.[2]

Finally, we point out that we should **start with digital education** as a first step for understanding NIS.

[1] *See https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/nis-in-education [accessed November 2012]*

[2] *Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Digital democracy on how ICT tools can change the relationship between citizens and governments http://europa.eu/rapid/press-release_SPEECH-12-738_en.htm [accessed October 2012]*

2 Introduction

ENISA works with different stakeholder groups to develop advice and recommendations on good practice in network and information security (NIS). It seeks to enhance existing expertise in EU Member States by supporting the development of **cross-border communities** (e.g. intermediaries for cyber-security) **committed to improving NIS** throughout the EU. This report aims to establish a link between these activities and education.

Since the beginning of 2011 ENISA has been working with Luxembourg on a small-scale project on the importance of **including recommendations from ENISA in educational curriculums**. At the end of 2012, the working group is still active. Several fruitful discussions have produced important results, which were published under the title: 'Network Information Security in Education: Consolidated ENISA contribution',[3] together with presentations and slides for educators. Furthermore, there was good collaboration between German-speaking countries to produce a revised '2013/14 Guide for Elementary Schools on Information Security' (see section 3.3.2 of this report).

This report is the result of work that is focused on ENISA deliverables, their reuse and insertion as educational materials by educators from the European Union. We acknowledge the existence of other bodies and initiatives[4] that deal with the safety, security and online behaviour of different target groups. The material proposed here can be considered as additional expertise towards the support of the end result: an educated digital citizen.

The main target group of our report is composed of educators, such as trainers, teachers, peers involved in formal education and non-formal education, including lifelong learning. **The significant role of educators must not be omitted from any ICT stakeholder map**!

This report presents a greater diversity of work than before, since we interacted with a larger number of experts through our survey and consultations and we also focused more on collaborative solutions.

This report comes with five information graphics (see section 8, Annex IV)[5] that were created with data from the report to provide handy summaries of key points and serve as multimedia material.

[3] *See https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/nis-in-education [accessed November 2012]*

[4] *For details see section 7, Annex III*

[5] *Please check www.enisa.europa.eu to see the graphics in expandable view*

3 The report

In recent years there have been many discussions on network and information security in education. Educators are, by nature, in a permanent learning process with new technologies to grasp, understand and use. One example of a plan to apply such technologies to the entire education system is the National Education Technology Plan (NETP)[6] from the USA, discussed here to provide a comparative example from overseas.

Figure 1 and Figure 2 show the complexity of the topic taken into account by the multidisciplinary working group behind the NETP. In Figure 1 the actors of 'A model of learning, powered by technology' are introduced, while in Figure 2 the services that empower the learning environment are mentioned. The same actors, factors and services are relevant in Europe and in fact globally, since the model overcomes geographical barriers.

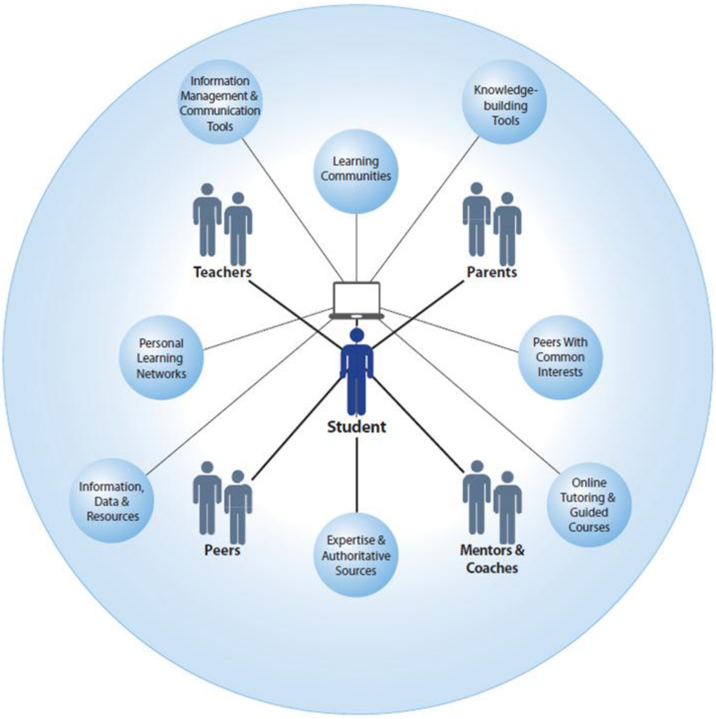
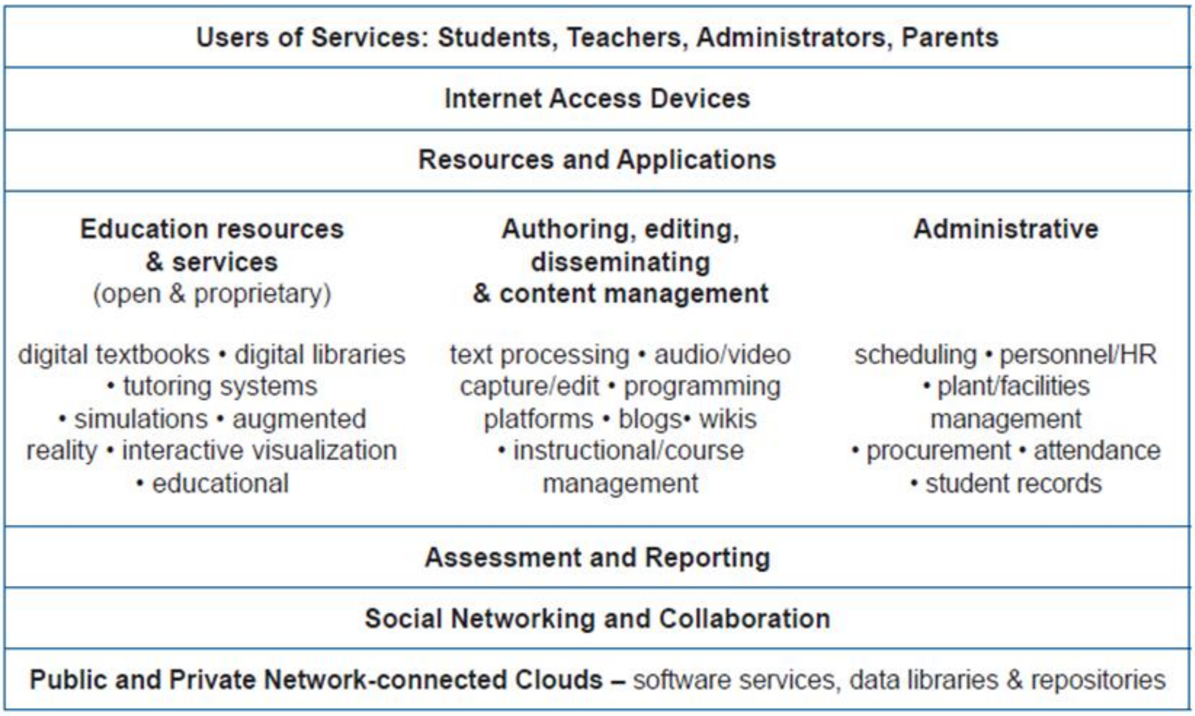

Information Management & Communication Tools
Knowledge-building Tools
Learning Communities
Teachers
Parents
Personal Learning Networks
Peers With Common Interests
Student
Information, Data & Resources
Peers
Expertise & Authoritative Sources
Mentors & Coaches
Online Tutoring & Guided Courses

Figure 1: Model of learning powered by technology (source: US NETP)

[6] *US Department of Education, Office of Educational Technology, 'Transforming American Education: Learning Powered by Technology', Washington, DC: http://www.ed.gov/technology/netp-2010 [accessed November 2012]*



Users of Services: Students, Teachers, Administrators, Parents

Internet Access Devices

Resources and Applications

Education resources & services (open & proprietary)	Authoring, editing, disseminating & content management	Administrative
digital textbooks • digital libraries • tutoring systems • simulations • augmented reality • interactive visualization • educational	text processing • audio/video capture/edit • programming platforms • blogs• wikis • instructional/course management	scheduling • personnel/HR • plant/facilities management • procurement • attendance • student records

Assessment and Reporting

Social Networking and Collaboration

Public and Private Network-connected Clouds – software services, data libraries & repositories

Figure 2: Framework for software services in a technology-empowered learning environment (source: US NETP)

The information from figures 1 and 2 is taken into consideration while working towards the objective of this ENISA report – to disseminate information management and communication tools for European learning communities.

3.1 Survey and consultations

The consultation phase started in July and resulted in nine online sessions with stakeholders involved at different levels in Member States from DE, ES, GR, IR, IT, NL, PL, RO, but also bodies like OWASP.[7]

The survey 'Network Information Security in Education: Key findings from practice' was open from the end of July until end of September, and was explicitly targeted at educators. It had seven open questions. The results are summarised below and supplemented by the infographics attached to this report (see Annex IV).

The respondents came from different backgrounds of NIS teaching: Secure Identification Technologies, OWASP Hacking-Lab initiative, Security audits following ISO/IEC 2700x standards Information security assessment and audit, Information Security, Information Technology Law, Personal Information security and Privacy awareness, Business: information

[7] *https://www.owasp.org/index.php/Main_Page [accessed November 2012]*

systems and information system security design and management, Incident Handling, Crisis Management, Business Continuity, Internal Fraud Management, Change Management, Work/Life Balance, eLearnSecurity, Machine Learning and Pattern Recognition techniques, ID-Cards, RFID Technology and Awareness.

The survey asked respondents to note elements that could be considered as part of a 'best session' structure. The results indicate that for a 'best session' an educator should take into account:

- Short introduction and hands-on labs;
- Stories and real-life examples;
- Full immersion training session, where training sessions may include: role playing activities, simulation/emulation exercises, teamwork & team-building activities, project management principles;
- Hacker contest: practical course in protection;
- Business game in place of exams;
- Mixture of videos;
- Structure of a presentation: 1. What do you know about the Internet? 2. Present the three parts of the presentation: Scam and virus, Privacy, and Internet Harassment; the proportion is: 20 minutes of theory, 30 minutes of practice and 10-20 minutes of question answering.

Asked which are the trends in teaching ICT, the replies suggest a wide range of topics such as:

- Labs;
- Cyber Physical Systems;
- Privacy and Trust, Cryptography;
- Software Security, Usable Security;
- Cloud Security, Internet and Infrastructure Security;
- International standards (e.g. ITIL, ISO/IEC 20000, ISO/IEC 27000);
- e-learning (e.g. Coursera), online testing via class server / blackboard solutions;
- Mobile learning;
- Mentoring sessions.

Educators register more requests for courses that result in international certifications for students.

Respondents commonly mentioned the need to promote awareness of personal information security and the need for legal advice on misbehaviours.

When asked which they consider to be the 'Top 10 challenges in ICT for students', the respondents mentioned:

- understanding what privacy means;
- understanding that use of technology implies risks and understanding that risks are not only personal, but can have an impact on other people as well (possibly very close to us);
- understanding that once information is published it is not likely to vanish from the Internet: a mistake today can impact the distant future;
- receiving adequate information and training from school, because new generations know and approach new technologies differently, and in some cases they have a better knowledge than their teachers;
- understanding technology, and not only using it;
- remapping real human relationships and behaviours on the internet: **Netiquette**;
- multidisciplinary expertise (legal, technical, organisational);
- filling the gaps between bytes, programming languages, and the role of ICT in modern society.

Respondents considered the following to be important elements of a successful partnership model for promoting net safety and security:

- ✓ Personal contact between user and lecturer;
- ✓ Accredited people with high skills, professional and experienced in the field;
- ✓ Continuously updated course material;
- ✓ Integrated usage of media and high quality supports;
- ✓ Flexible structure of courses;
- ✓ Cooperation with industry and academia;
- ✓ A 'can do' attitude and openness to change; colloquial teaching;
- ✓ Passion and experienced communication;
- ✓ High ethical standards;
- ✓ Professionalism and experience in the field, real cases discussed;
- ✓ 'Not giving them the fish but teaching them how to fish':[8] offering the model, not just providing the solution without some hard work;
- ✓ Public and private cooperation to finance web resources;
- ✓ Train the trainers.

(Annex II contains some resources recommended by the respondents as further reading.)

[8] *Quote from a survey respondent*

3.2 ENISA recommendations from 2012 reports

This part of the report contains recommendations extracted for educators from 2012 ENISA reports.

3.2.1 'Privacy considerations of online behavioural tracking'

What is behavioural tracking?

Internet users are being increasingly tracked and profiled and their personal data are extensively used as currency in exchange for services.

It is important that this new reality is better understood by all if we are to be able to support and respect the right for privacy.

Behavioural targeting is the practice of tailoring online content, especially advertisements, to visitors based on their inferred interests, or 'profile'. The process of constructing this profile using data mining – transforming data into knowledge – is known as online behavioural profiling. The underlying data is typically a log of the user's web activity, and the data collection process is called behavioural tracking.

For example, Facebook tracks across sites via its 'Like' button; each time a user visits a site that contains a Facebook 'Like' button, Facebook is informed about it, even if the user does not click on this button.

Tracking techniques include: cookies, JavaScript, Super cookies and Ever cookies, Browser fingerprints, Location tracking.

What are the dangers of tracking?

One of the biggest risks of tracking is global surveillance. This surveillance can be performed by government, for security or political reasons, or by companies for commercial reasons. Another consequence of tracking and profiling is service discrimination or exclusion. Profiling is often used by service providers to personalise their content to users.

What can be done about tracking?

The report identifies several types of existing consumer education efforts in the area of online tracking:

- General advice about online privacy and raising awareness of the existence of the online tracking ecosystem;
- Initiatives to inform consumers about self-defence tools. Innumerable websites exhort consumers to periodically clear cookies and provide instructions for doing so. Stanford's donottrack.us and Mozilla's Do Not Track page both provide information on how to enable Do Not Track and what it will and will not do;
- Provision of information about the data collection practices of specific companies and their products in the online tracking ecosystem.

It is also worth noting that numerous experimental results in the area of privacy research indicate that the prime interests for the majority of users of online services are:

- convenience / ease of use, and
- cost of service (with a preference for 'free' offers).

Obviously both of these requirements imply the necessity for users to give away to the service providers personal information that is monetised by the providers in exchange for the 'free' services offered.

For the full report please visit: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking

3.2.2 'Study on monetising privacy. An economic model for pricing personal information'

What does 'monetising privacy' mean?

'Monetising privacy' refers to a consumer's decision regarding disclosure or non-disclosure of personal data in relation to a purchase transaction.

Consumers benefit from personalisation of products on the one hand, but might be locked in to services on the other. Moreover, personalisation also bears a privacy risk, i.e. that data may be compromised once disclosed to a service provider.

Recommendations from the report

Users should be provided with options that allow them to disclose less personal data. Since such differentiation might lead to higher service prices, the EU regulatory framework should be sufficiently flexible to allow differentiation between service providers, enabling comparison of prices and requiring market players to offer privacy-friendly services.

For the full report please visit:

www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy

3.2.3 'To log or not to log? – Risks and benefits of emerging life-logging applications'

What is 'life-logging'?

While the term 'life-logging' might be new, the practices and activities it represents are well known, well established and pervasive historically and currently in societies. The keeping of a diary, the writing of a biography or autobiography, personal accounts of historical moments (sporting, war) and news stories capturing moments of celebrities' lives can all be represented in life-logging.

Benefits for individuals

Individuals can benefit from life-logging, both on a personal level and on a societal level. Life-logging allows people to stay in closer contact with one another regardless of physical distance. This may reduce their sense of isolation and help them enjoy social bonds with others in the virtual world.

From a professional perspective, individuals can be more aware of their colleagues' and professional contacts' activities, which may make it easier to contact the right people from their networks when they need advice on a specific problem; they can also benefit professionally by building their reputation online

What does the report contain?

The scenario can briefly be summarised a day in the life of a family, 3-5 years from now, with 2 adults (Annika and Bennie), 2 young people (Christer and Dana) who to greater or lesser degrees make use of different life-logging and related services during the course of their respective daily routines. It captures all four and other individuals interacting with them in a variety of settings, performing a number of everyday activities, including work, commuting, attending school and relaxing at home. During the course of their daily activities all of them also come into contact with other individuals, commercial providers as well as government agencies. In these various interactions as well as through the activities of the family, it is clear that life-logging is embedded within their daily routines. By illustrating these routines, the scenario illuminates the wide variety of risks that this report considers.

Recommendations for individuals

We believe that being an informed user is the first step: the right to be forgotten, the right to be left alone, etc., are probably best enforced if the user is in control over his/her personal data. Specifically, we recommend that individuals:

- although the industry and the state /government and EU institutions have the most important role to play in this, be alert in protecting their own privacy (for example by making use of available tools) and be aware of the potential impacts on others, accidentally or deliberately affected by their own use of these services, as well as the impacts on themselves by the use of such services by others;

- make use of privacy-friendly tools and consider factors and variables that reflect the trade-offs they have to make between the benefits (e.g. gain in convenience, increased functionality, discounts) and risks (e.g. mistrust, disadvantages, risk of misuse or manipulation).

For the full report please visit:

http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/life-logging-risk-assessment/to-log-or-not-to-log-risks-and-benefits-of-emerging-life-logging-applications

3.3 Study cases from Member States

This section introduces the work done by the partners from three Member States (Austria, Luxembourg and Denmark) involved in the working group established in 2011 and still active in 2012.

3.3.1 NIS in education as part of the Austrian Cyber Security Strategy[9]

National ICT Security Strategy Austria

In 2011 the Federal Chancellery of Austria (Österreichisches Bundeskanzleramt, BKA) initiated the development of Austria's National ICT Security Strategy (Nationale IKT-Sicherheitsstrategie Österreich). The aim was to assess the current situation and to develop a proactive concept to protect cyberspace and human beings in this virtual space by taking into account their fundamental rights and freedoms.

130 experts from industry, science and public administration participated in the development of this strategy. Starting with a kick-off-meeting in November 2011, five working groups were established to deal in-depth with the various aspects of cyber-security – from awareness raising to specific counter-actions against security incidents. The results of the five working groups – 'Stakeholders and Structures', 'Critical Infrastructure', 'Risk Management and Situation Assessment', 'Education and Research' and 'Awareness' – were integrated into an overall strategy and presented in June 2012.

The Austrian National ICT Security Strategy identifies 23 strategic aims and 55 measures to ensure and enhance security in cyberspace. The results are to be integrated with the Austrian Strategies on Cyber Defence and Cyber Crime in 2013.

The working group on 'Education and Research'

While it is evident that a national security strategy deals with the protection of critical infrastructures, risk management or stakeholders, it is **interesting to note that education and research formed a significant part of the overall strategy**. The fact that there was a specific working group dedicated to these topics indicates the importance of having a sound basis of knowledge and skills in information security and cyber-security, both on the expert level and at the broad level of citizens and users of all ages.

The working group dealt with three main items:

- network and information security (NIS) in primary and secondary education;
- study and training programmes – offered as specialisation of general ICT studies as well as specific ICT security studies – with a focus on security at tertiary level;
- Strengthening research in ICT and information security.

[9] *Contribution by Prof. Ingrid Schaumueller-Bichl, member of the working group on 'Education and Research'.*

Discussions in the working group showed a strong need for NIS in education even for the youngest groups – children in primary and secondary schools, not forgetting teachers and parents.

The working group identified in total seven strategic aims, three of them dealing specifically with NIS in education. These three aims were as follows:

Education in ICT, ICT security and media competence in early school grades:

Attacks on ICT infrastructures through inadequately protected private systems as well as the individual's loss of privacy may be prevented on a long-term basis only if citizens have a wider understanding of ICT security and adequate skills in using the new media. This understanding needs to be developed at school as early as possible.

ICT and ICT security must be incorporated to a greater extent into school curriculums and daily teaching practice from primary school level onwards. It is a medium-term goal that each individual's familiarity with the use of modern media can be taken for granted – this is not only in the interest of the citizens but also the basis for protecting national infrastructures.

Dealing with new technologies in a competent and secure way has to become an integral part of education in all types of schools. As children interact with new media at a very young age this issue must be addressed even at primary-school level and reinforced in secondary schools. Educational standards should be defined to ensure adequate level of competence in all school types.

Education in ICT and ICT security for all teachers:

Schools will not succeed in teaching a creative, safe and critical approach to ICT and new media unless teachers receive adequate training.

Providing children with the skills for the constructive and secure handling of ICT and new social media requires teachers to be familiar with the subject and the new developments and to have profound and up-to-date knowledge on the subject. ICT and ICT security should become an integral part of the training of all future teachers during their university studies, regardless of their main subject. Continuing education and training has to be provided for teachers already in the field.

Special programs for parents:

Parents often hesitate to discuss the use of modern technologies with their children, believing that young people have more skills in this area. Yet it is important that parents are able to question critically the way their children handle new media and to help them understand the opportunities and risks of the modern technologies. Special programmes have to be developed for parents within the school system which will help them to become a knowledgeable source of advice for their children and to examine their use of new media and media skills.

Next steps:

As next steps specific measures and concrete actions will be derived from the strategic aims identified in the National ICT Security Strategy. The discussions in the working group showed that there is much material available and many highly interesting activities are going on. Yet, those activities are usually restricted to specific types of education or specific schools, often based on the personal involvement of dedicated teachers. It will be necessary to define an agreed level of minimum knowledge to be reached in the various stages of education. In the next steps it will be important to involve all relevant stakeholders to integrate NIS education in schools and also to make it part of a lifelong learning process.

As a first step relevant material concerning NIS in education will be integrated into an ICT security platform that will be set up in Austria during the coming months. In this platform specific information will be provided for target groups, comprising children, parents, teachers, people of 60+, but also institutions such as companies, the research and technology sector and public administration. This platform will serve as a means to exchange and spread information among all stakeholders. ENISA's material on NIS in education will be integrated as a valuable part of this information.

3.3.2 Revised 2013/14 'Information Security Guide for Use in School and at Home' Luxembourg[10]

Background

The so called 'Leitfaden zur Informationssicherheit für den Unterricht und für zu Hause' (Information Security Guide for Use in School and at Home) published in 2010 was a tremendous success, and received a very positive feedback. The guide, issued by the Ministry of Economy and the Ministry of National Education, was based on the knowledge acquired in hundreds of classroom training courses involving more than 25,000 Luxembourgish children and teenagers since 2007. The authors' constant interactions with the pupils in the classroom enabled them to publish a highly appreciated tool in the field of information security.

However, over the last 12 months, the authors have felt a need to review the visual presentation of the valuable content, especially concerning the practical features ('ready-to-use elements') in this guide.

[10] *Contribution by Albin Wallinger on behalf of the project team in Luxembourg.*

Objective

The broader goal was to find a **new didactic approach and to give the educators a significantly revised 'workbook' full of fresh and practical elements** that would really 'kindle their enthusiasm' for information security topics.

Method

In September 2012 the authors conducted qualitative research to gather feedback on a variety of design parameters. A total of 20 elementary school teachers were interviewed in different locations. They were asked to look through the current Guide and its 62 pages and 12 appendices and to evaluate 3 new design options for a better visual presentation.

After looking through the pages, the educators were asked to recall, without any prompts, the elements that helped them most in their classroom teaching. On this measure ('Highly helpful, ready-to-use') some elements performed well, some not so well. With the alternative layout options in view, the educators were asked how much they liked various alternative layout concepts (concepts A, B, C).

Results

In terms of didactic features, all the elements that were meant to make information security come alive (real-life stories, quizzes, worksheets) were well received. Concerning the layout concept options, the educators responded favourably to the **'textbook-atlas-concept'**, stating that it was consistent with the daily challenges in the classroom.

In the 'textbook-atlas-concept', the lessons are described both in words (on the left side of a double page) and shown in didactically useful worksheets (on the right side of the double page).

It should be noted that the results from this research are consistent with learning obtained in German publishing houses focusing on elementary school teachers and, more generally speaking, with studies in the field of 'information design' and 'visual presentation of complex content'.

Conclusions

Based upon the results, the challenge to the authors and designers of the new Guide will not only be 'to create templates that look better' as far as the educators are concerned, but to make many pages more 'action-oriented'. As a consequence, the new Guide will include more than 30 innovative activity sheets (in A4 format) which can be easily copied and used in classroom teaching. Educators can thus extend the lessons by letting children discuss the sheets and carrying out the activities. Thanks to this approach the worksheets can be used as a source of very interesting and instructive activities.

Concerning the content, the revised Guide will replace some lessons with several new and updated lessons that address the latest research and developments in the field of information security in greater depth.

Next steps

The relaunched version of the 'Information Security Guide for Use in School and at Home' will be published in autumn 2013 (in the German language). The guide will also be distributed in partnership with a German and an Austrian partner organisation and thus be made available in a printed version in a total of three countries (Luxembourg, Germany, and Austria). The content of the guide, including the Activity Sheets, will also be made available in online form to the ENISA partners. The revised Guide will fit strategically within the activities of the Luxembourg government and perpetuate and strengthen the efforts of the Grand-Duchy of Luxembourg in the field of information security.

3.3.3 Recommendation to educators from the authors of 'Fake It'[11]

This section is based on the book *Fake It – Your Guide to Digital Self-Defense*,[12] and it introduces new content and our discussion with the authors.

> *Kolding, a mid-size town in the Danish province of Jutland, can proudly call itself a first mover. It is not only posting cultural events and city services on their Facebook page, it is also maintaining an active dialogue with its citizens, who are pleased they can reach their city on Facebook – where over half of the Danish population is said to have an account.*
>
> *But by nudging even more Danes to join Facebook, the city is pushing them to expose their private lives to the data mining efforts of a for-profit company based in the U.S. On Kolding's page, citizens 'like' posts about chlamydia, telling that their spouse is a heavy smoker or revealing that they receive social services. Kolding does state in their 'about' page that it doesn't do casework over Facebook. But it is not warning citizens against leaving sensitive personal data on the commercial network whose business model revolves around gathering and selling personal data.*
>
> *A public school in Hellerup, North of Copenhagen, is just as happy with Facebook. Here, children in seventh grade cannot participate in the homework unless they have a*

[11] *authors Pernille Tranberg and Steffan Heuer*

[12] http://www.digital-selfdefense.com/ *Fake It – Your Guide to Digital Self-defense* is a thorough walk-through of the risks individual consumers and citizens take when they live life online. The book describes how users' personal data is collected, stored, mined and abused by commercial companies. But it also shows how the individual can participate and be active on social media and the Internet in general while at the same time protecting their online identity and reputation 'Fake It' lists a whole range of great tools to retain control over users data [accessed November 2012]

Facebook account. The class has a group where the pupils upload their homework, including large video files, have discussions, and receive messages from the teacher about homework. The school has its own intranet, but it is slow, not dynamic enough, and you cannot upload large files. The school has established principles about the usage of social networks such as teachers not being friends with the pupils, and they also discuss web ethics. But they have no discussion about the consequences of exposing the enrolled children's personal data on Facebook.

The city of Kolding and the school in Hellerup are no isolated cases or exceptions. State-run institutions all over Scandinavia are using social media like Facebook without any privacy considerations. We're talking about schools, cities and even the police. The reason might be that they view Facebook as a social infrastructure, not as a commercial company. Further, they argue that they have to be where many of their citizens already are.

Some cities are still hesitating to embrace Facebook. But the reason is economics, not concerns over privacy or data mining. The hold-outs are afraid that 'going social' will cost them more time and money than it saves them. Unfortunately, they are not holding back because of the really worrisome issue: the big business of personal data.

The debate about these risks of losing control over one's data online and how to perform digital self-defence has – up to now – not been very lively, at least in Northern Europe. Educators play an important role in pushing this discussion. There is nothing wrong about a person's individual choice to share everything about themselves, as long as they know what they are doing and acknowledge the risks their acts entail. To do so as a child or teenager, without informed consent, is a different matter however.

Citizens in modern societies risk paying a huge price for their voluntary and involuntary oversharing. We suffer from very unhealthy data emissions. No wonder that some privacy experts compare the current situation to the environmental pollution of the 1950s and 60s, when humans poisoned and destroyed their ecosystem without thinking about it and many large companies denying it. It led to the rise of the environmental movement, heightened concern and stringent laws, yet we are still paying the price for our initial negligence.

Today, we are polluting our networked world with our personal data, oblivious to the risks for ourselves and our children. Personal data has become the currency that makes the digital economy go round. Our habits, hobbies and hidden secrets have become commoditized, and companies earn billions at our expense when we sign up for and use supposedly 'free' services.

Educators have a special obligation to inform citizens and consumers about the risks of exposing their personal data. Young people need to learn how to keep the pieces of their digital persona to themselves and work with multiple identities. They should 'fake it' online in as many situations as possible when they are not acting professionally.

It's not that strange an idea. When very young, children already learn to play with several identities. In game settings such as Habbo Hotel, MovieMaker, The Sims, World of Warcraft and others, they are already using aliases and fake names. All of their friends know who they are anyhow. Children have no problems navigating their world under various roles and pseudonyms. Then, when they want to join Facebook for the first time, they are suddenly forced to giving one company all their personal data. The social network tries to enforce a 'real name policy' and threatens to close down accounts if they find out a user has signed up with a fake name.

Such a real name mandate is neither legitimate nor legal, at least in countries with progressive data protection laws. German authorities, for instance, are instructing their pupils to fake it on Facebook and other social media platforms. We couldn't agree more.

Neither children nor grownups can foresee what their postings can be used for in five or ten years. The Internet does not forget or let trivial details gracefully fade away. As humans we know that contexts are constantly changing – and so are our mood and opinions. A server for a social network is not that discerning or forgiving. Many people already regret some of their posts, but once it's out there, it cannot be deleted. It stays on some record that can mined by commercial entities, governments or potential employers.

Finally, if everybody ends up being transparent and being 100 percent under the surveillance of governments and commercial entities, we will end up living in a world of participatory authoritarianism. You are forced to make yourself machine readable or risk being cast out. It is up to educators and their pupils to defend the rights to their data today.

In summary, faking it online is one great tool to protect your identity in the digital world. It is arguably a rather primitive tool today, but the area of digital self-defense is ripe for innovation and more tools and services to manage multiple identities will soon be launched. Still, ***using pseudonyms and aliases on the Internet is only a first step****. You need to use many other tools, particularly browser extensions to block literally hundreds of companies from tracking you everywhere you go, on the web and with your mobile*.

To find out more about the digital footprint and advanced tools see the Electronic Frontier Foundation report 'How Unique Is Your Web Browser?' and ENISA's report 'Study on data collection and storage in the EU'.[13]

[13] 'How Unique Is Your Web Browser?' by Peter Eckersley: http://panopticlick.eff.org/browser-uniqueness.pdf and 'Study on data collection and storage in the EU': https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection [accessed November 2012]

4 Conclusions

This report intends to provide useful information that should be immediately applicable in practice. It also aims to encourage readers, whether educators or students, to adopt a **'can do' attitude** to enhancing their information security.

From the survey and online consultations educators should choose the information that most suits their objectives and apply it accordingly. We also invite you to send us **your observations** and experience from practice if you want to add essential data for future initiatives on the topic.

The recommendations taken from ENISA's 2012 reports should be considered as supplementary material (remember that one can always check ENISA's website[14] for updates). As ENISA is a body of expertise for network information security, the interested reader can find valuable information, technical or for general use, that brings an important added value.

With the case studies introduced, the report brings its contribution to the exchange of information between Member States.

Among the most important recommendations of the report are:

- cyber-security strategies should include a subsection on education and research as part of the overall strategy;
- the need to promote awareness regarding personal information security and for legal advice on misbehaviours;
- the new didactic approach and 'textbook-atlas-concept' should be used for NIS guides;
- using pseudonyms and aliases on the Internet is a first step in protecting your personal data.

To conclude, essential information can only be disseminated to the target users when all stakeholders get involved. From beginning of 2011 and throughout 2012, ENISA's key role in this area has been to discuss harmonised education curriculums with Member States. We hope that the work will achieve its objectives by stepping up national efforts on NIS education and training, together with ENISA involvement.

[14] www.enisa.europa.eu

5 Annex I: References

- [1] ENISA report 'Network Information Security in Education: Consolidated ENISA contribution' https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/nis-in-education accessed November 2012;
- [2] Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda Digital democracy: how ICT tools can change the relationship between citizens and governments: http://europa.eu/rapid/press-release_SPEECH-12-738_en.htm accessed October 2012;
- [5] US Department of Education, Office of Educational Technology, Transforming American Education: Learning Powered by Technology, Washington, DC: http://www.ed.gov/technology/netp-2010 accessed November 2012'
- ENISA report 'Privacy considerations of online behavioural tracking' http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking accessed November 2012;
- ENISA report 'Study on monetising privacy. An economic model for pricing personal information' http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy accessed November 2012;
- ENISA report 'To log or not to log? – Risks and benefits of emerging life-logging applications' http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/life-logging-risk-assessment/to-log-or-not-to-log-risks-and-benefits-of-emerging-life-logging-applications accessed November 2012;
- *Fake It – Your Guide to Digital Self-Defense*, by Pernille Tranberg and Steffan Heuer http://www.digital-selfdefense.com accessed October 2012;
- Electronic Frontier Foundation report, 'How Unique Is Your Web Browser?' by Peter Eckersley http://panopticlick.eff.org/browser-uniqueness.pdf accessed November 2012;
- ENISA report 'Study on data collection and storage in the EU' https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection accessed November 2012

6 Annex II: Resources recommendend by survey respondents

The survey ‘Network Information Security in Education: key findings from practice’, resources recommended:

- ENISA website www.enisa.europa.eu
- The Open Web Application Security Project www.owasp.org; www.hacking-lab.com;
- *Introduction to Cryptography* (2nd edn), by Johannes Buchmann; ISBN10: 0387207562;
- General websites: Standard ISO, websites of public authorities, IS association and newsletter, IS courses and training, IS certifications vendor neutral, ISACA chapter www.isaca.org;
- Italian Clusit, Crypto-gram www.schneier.com;
- Blog https://SecAtSchool.wordpress.com;
- NIST http://www.nist.gov/itl/csd/mobile-103112.cfm and OWASP guidelines https://www.owasp.org/index.php/OWASP_Guide_Project ;
- SANS reading room material http://www.sans.org/reading_room/ ;
- Web of knowledge, Thomson Reuters http://wokinfo.com/;
- ISECOM http://www.isecom.org/home.html;
- Spain resources: www.osi.es (for end users); www.menores.osi.es (for age groups 5-8, 9-12, 13-17, parents and educators); www.pantallasamigas.com (teenagers); www.deaquinopasas.org (Save The Children)(Teenagers); www.protecciononline.com (children and parents); http://www.youtube.com/osimenores, http://www.youtube.com/osiseguridad; The social media channels: http://www.facebook.com/osiseguridad and https://twitter.com/osiseguridad focused in final users; The social media channels: http://www.facebook.com/piensoluegoclico and http://www.tuenti.com/piensoluegoclico focused on young people;
- *Security in Computing* (4th edn), by Shari Lawrence Pfleeger, Charles P. Pfleeger, ISBN:9788131727256 http://www.pearsoned.co.in/web/books/9788131727256_Security-in-Computing_Shari-Lawrence-Pfleeger.aspx;

7 Annex III: Useful websites for NIS Education

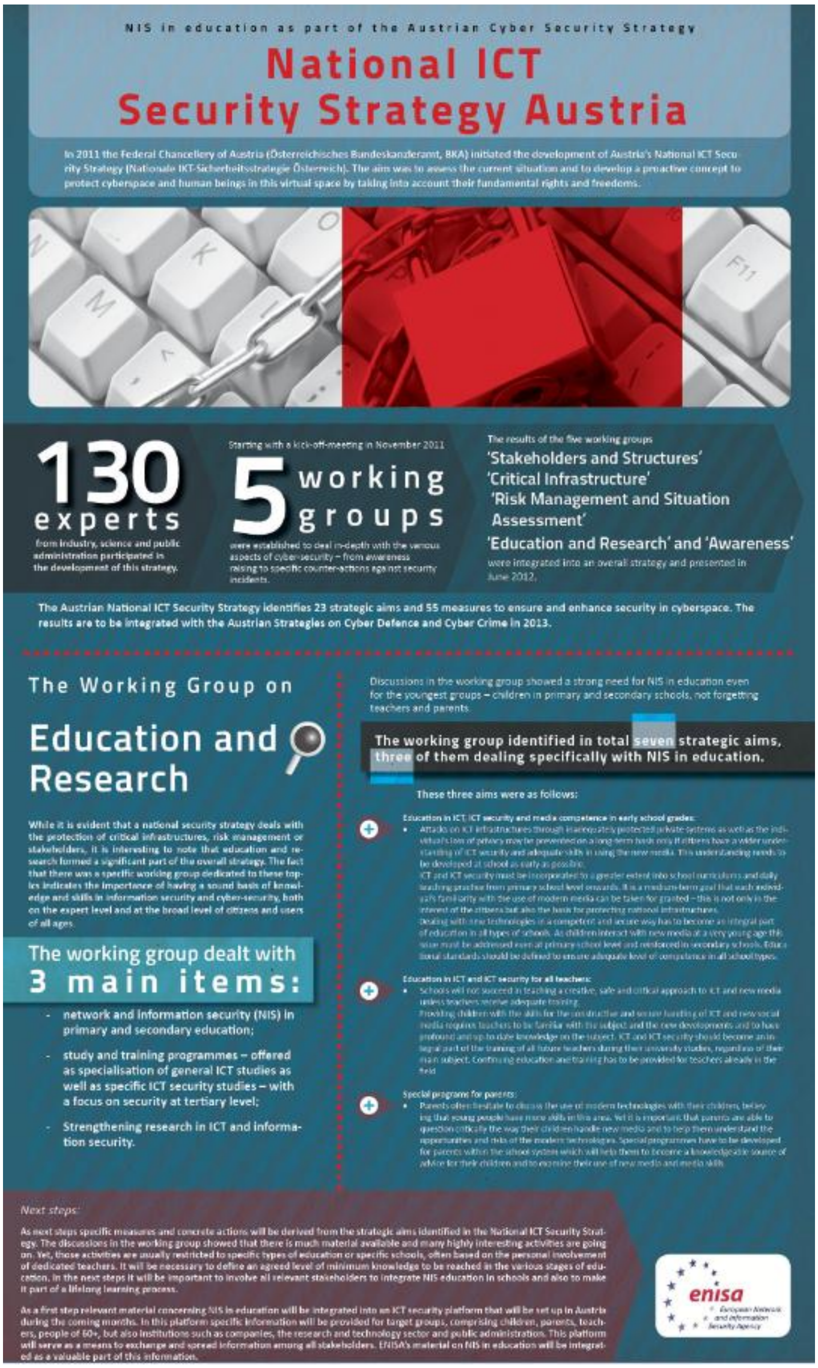
These resources were last accessed in November 2012:

- Europe’s Information Society thematic portal http://ec.europa.eu/information_society/activities/sip/index_en.htm
- EU KIDS online work http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx
- INHOPE http://www.inhope.org/gns/home.aspx
- INSAFE http://www.saferinternet.org/web/guest/home;jsessionid=B160C5B8BC0CEF85583C3991CAD6CDF8
- EURYDICE http://eacea.ec.europa.eu/education/eurydice/index_en.php
- South West Grid for Learning http://www.swgfl.org.uk/About-Us/About-Us
- ITU http://www.itu.int/ITU-D/youth/
- COE www.coe.int

8 Annex IV: Information graphics

To obtain these graphics in an expandable format please check the ENISA website.

1.



NIS in education as part of the Austrian Cyber Security Strategy

National ICT Security Strategy Austria

In 2011 the Federal Chancellery of Austria (Österreichisches Bundeskanzleramt, BKA) initiated the development of Austria's National ICT Security Strategy (Nationale IKT-Sicherheitsstrategie Österreich). The aims was to assess the current situation and to develop a proactive concept to protect cyberspace and human beings in this virtual space by taking into account their fundamental rights and freedoms.

130 experts from industry, science and public administration participated in the development of this strategy.

Starting with a kick-off-meeting in November 2011 **5 working groups** were established to deal in-depth with the various aspects of cyber-security – from awareness raising to specific counter-actions against security incidents.

The results of the five working groups
'Stakeholders and Structures'
'Critical Infrastructure'
'Risk Management and Situation Assessment'
'Education and Research' and 'Awareness'
were integrated into an overall strategy and presented in June 2012.

The Austrian National ICT Security Strategy identifies 23 strategic aims and 55 measures to ensure and enhance security in cyberspace. The results are to be integrated with the Austrian Strategies on Cyber Defence and Cyber Crime in 2013.

The Working Group on

Education and Research

While it is evident that a national security strategy deals with the protection of critical infrastructures, risk management or stakeholders, it is interesting to note that education and research formed a significant part of the overall strategy. The fact that there was a specific working group dedicated to these topics indicates the importance of having a sound basis of knowledge and skills in information security and cyber-security, both on the expert level and at the broad level of citizens and users of all ages.

The working group dealt with **3 main items:**

- network and information security (NIS) in primary and secondary education;
- study and training programmes – offered as specialisation of general ICT studies as well as specific ICT security studies – with a focus on security at tertiary level;
- Strengthening research in ICT and information security.

Discussions in the working group showed a strong need for NIS in education even for the youngest groups – children in primary and secondary schools, not forgetting teachers and parents.

The working group identified in total seven strategic aims, three of them dealing specifically with NIS in education.

These three aims were as follows:

Education in ICT, ICT security and media competence in early school grades:

- Attacks on ICT infrastructures through inadequately protected private systems as well as the individual's loss of privacy may be prevented on a long-term basis only if citizens have a wider understanding of ICT security and adequate skills in using the new media. This understanding needs to be developed at school as early as possible.
  ICT and ICT security must be incorporated to a greater extent into school curriculums and daily teaching practice from primary school level onwards. It is a medium-term goal that each individual's familiarity with the use of modern media can be taken for granted – this is not only in the interest of the citizens but also the basis for protecting national infrastructures.
  Dealing with new technologies in a competent and secure way has to become an integral part of education in all types of schools. As children interact with new media at a very young age this issue must be addressed even at primary school level and reinforced in secondary schools. Educational standards should be defined to ensure adequate level of competence in all school types.

Education in ICT and ICT security for all teachers:

- Schools will not succeed in teaching a creative, safe and critical approach to ICT and new media unless teachers receive adequate training.
  Providing children with the skills for the constructive and secure handling of ICT and new social media requires teachers to be familiar with the subject and the new developments and to have profound and up-to-date knowledge on the subject. ICT and ICT security should become an integral part of the training of all future teachers during their university studies, regardless of their main subject. Continuing education and training has to be provided for teachers already in the field

Special programs for parents:

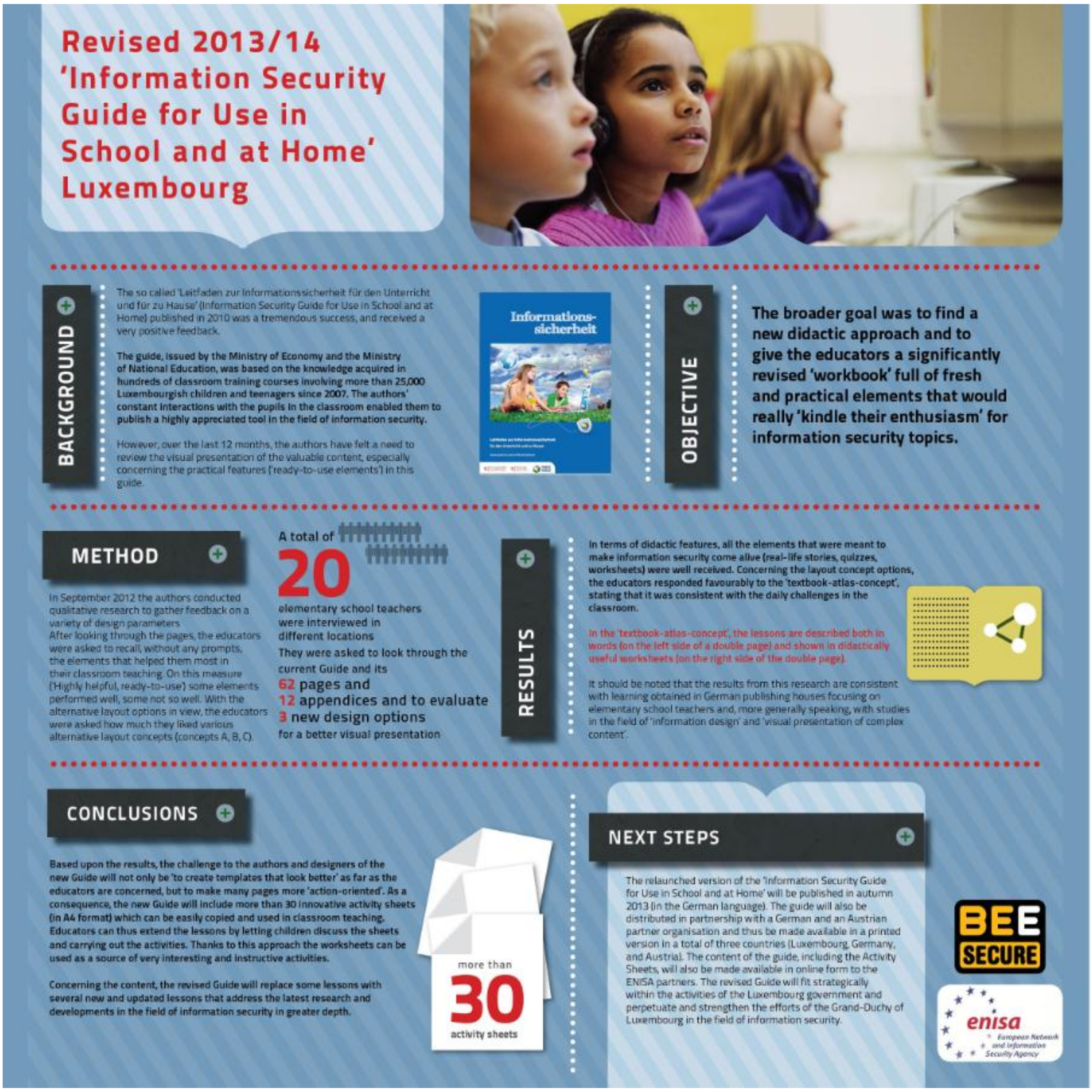
- Parents often hesitate to discuss the use of modern technologies with their children, believing that young people have more skills in this area. Yet it is important that parents are able to question critically the way their children handle new media and to help them understand the opportunities and risks of the modern technologies. Special programmes have to be developed for parents within the school system which will help them to become a knowledgeable source of advice for their children and to examine their use of new media and media skills.

Next steps:

As next steps specific measures and concrete actions will be derived from the strategic aims identified in the National ICT Security Strategy. The discussions in the working group showed that there is much material available and many highly interesting activities are going on. Yet, those activities are usually restricted to specific types of education or specific schools, often based on the personal involvement of dedicated teachers. It will be necessary to define an agreed level of minimum knowledge to be reached in the various stages of education. In the next steps it will be important to involve all relevant stakeholders to integrate NIS education in schools and also to make it part of a lifelong learning process.

As a first step relevant material concerning NIS in education will be integrated into an ICT security platform that will be set up in Austria during the coming months. In this platform specific information will be provided for target groups, comprising children, parents, teachers, people of 60+, but also institutions such as companies, the research and technology sector and public administration. This platform will serve as a means to exchange and spread information among all stakeholders. ENISA's material on NIS in education will be integrated as a valuable part of this information.

2.



Revised 2013/14 'Information Security Guide for Use in School and at Home' Luxembourg

BACKGROUND

The so called 'Leitfaden zur Informationssicherheit für den Unterricht und für zu Hause' (Information Security Guide for Use in School and at Home) published in 2010 was a tremendous success, and received a very positive feedback.

The guide, issued by the Ministry of Economy and the Ministry of National Education, was based on the knowledge acquired in hundreds of classroom training courses involving more than 25,000 Luxembourgish children and teenagers since 2007. The authors' constant interactions with the pupils in the classroom enabled them to publish a highly appreciated tool in the field of information security.

However, over the last 12 months, the authors have felt a need to review the visual presentation of the valuable content, especially concerning the practical features ('ready-to-use elements') in this guide.

OBJECTIVE

The broader goal was to find a new didactic approach and to give the educators a significantly revised 'workbook' full of fresh and practical elements that would really 'kindle their enthusiasm' for information security topics.

METHOD

In September 2012 the authors conducted qualitative research to gather feedback on a variety of design parameters
After looking through the pages, the educators were asked to recall, without any prompts, the elements that helped them most in their classroom teaching. On this measure ('Highly helpful, ready-to-use') some elements performed well, some not so well. With the alternative layout options in view, the educators were asked how much they liked various alternative layout concepts (concepts A, B, C).

A total of
20
elementary school teachers
were interviewed in
different locations
They were asked to look through the
current Guide and its
62 pages and
12 appendices and to evaluate
3 new design options
for a better visual presentation

RESULTS

In terms of didactic features, all the elements that were meant to make information security come alive (real-life stories, quizzes, worksheets) were well received. Concerning the layout concept options, the educators responded favourably to the 'textbook-atlas-concept', stating that it was consistent with the daily challenges in the classroom.

In the 'textbook-atlas-concept', the lessons are described both in words (on the left side of a double page) and shown in didactically useful worksheets (on the right side of the double page).

It should be noted that the results from this research are consistent with learning obtained in German publishing houses focusing on elementary school teachers and, more generally speaking, with studies in the field of 'information design' and 'visual presentation of complex content'.

CONCLUSIONS

Based upon the results, the challenge to the authors and designers of the new Guide will not only be 'to create templates that look better' as far as the educators are concerned, but to make many pages more 'action-oriented'. As a consequence, the new Guide will include more than 30 innovative activity sheets (in A4 format) which can be easily copied and used in classroom teaching. Educators can thus extend the lessons by letting children discuss the sheets and carrying out the activities. Thanks to this approach the worksheets can be used as a source of very interesting and instructive activities.

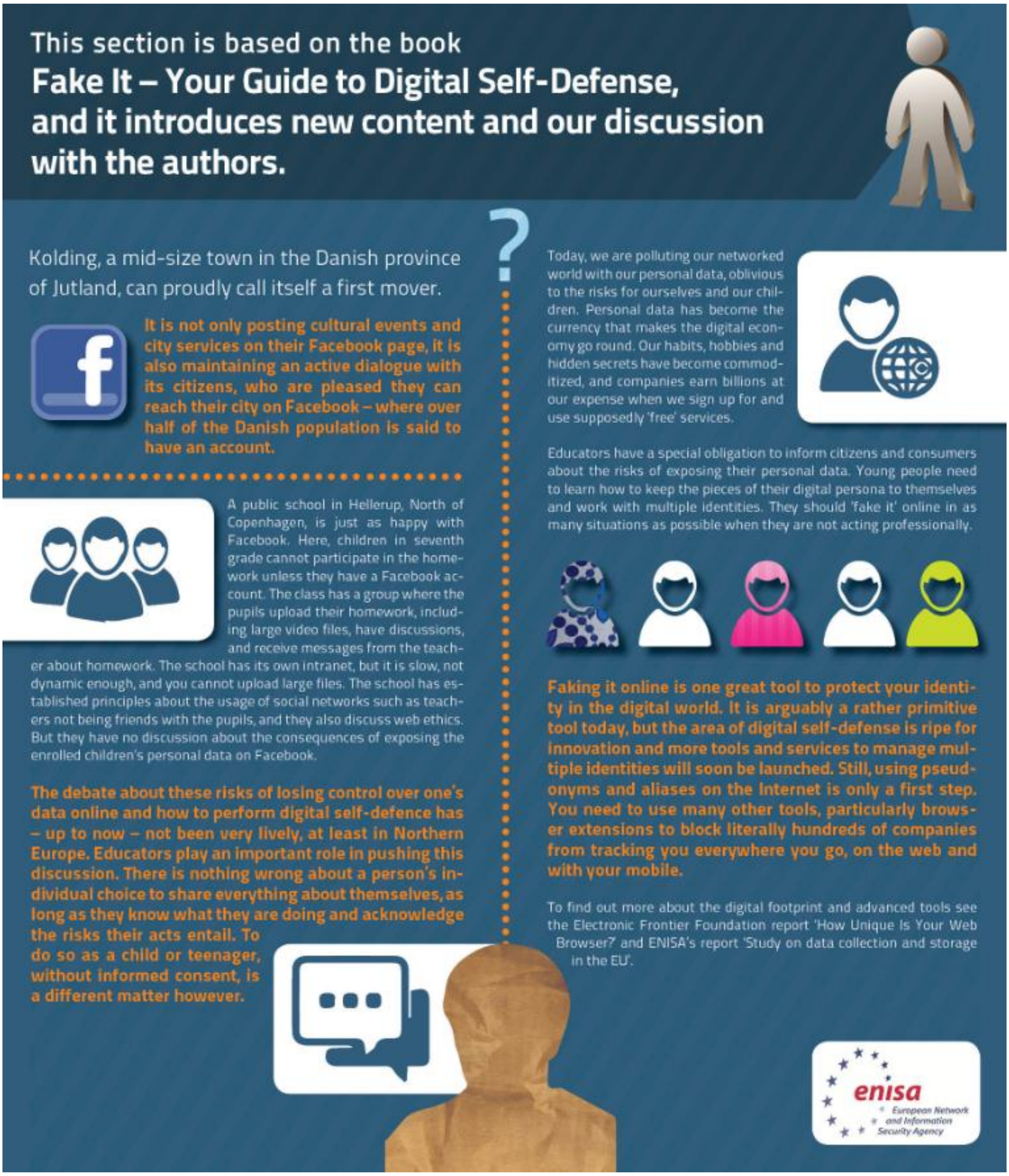
Concerning the content, the revised Guide will replace some lessons with several new and updated lessons that address the latest research and developments in the field of information security in greater depth.

more than
30
activity sheets

NEXT STEPS

The relaunched version of the 'Information Security Guide for Use in School and at Home' will be published in autumn 2013 (in the German language). The guide will also be distributed in partnership with a German and an Austrian partner organisation and thus be made available in a printed version in a total of three countries (Luxembourg, Germany, and Austria). The content of the guide, including the Activity Sheets, will also be made available in online form to the ENISA partners. The revised Guide will fit strategically within the activities of the Luxembourg government and perpetuate and strengthen the efforts of the Grand-Duchy of Luxembourg in the field of information security.

3.



This section is based on the book

Fake It – Your Guide to Digital Self-Defense, and it introduces new content and our discussion with the authors.

Kolding, a mid-size town in the Danish province of Jutland, can proudly call itself a first mover.

It is not only posting cultural events and city services on their Facebook page, it is also maintaining an active dialogue with its citizens, who are pleased they can reach their city on Facebook – where over half of the Danish population is said to have an account.

A public school in Hellerup, North of Copenhagen, is just as happy with Facebook. Here, children in seventh grade cannot participate in the homework unless they have a Facebook account. The class has a group where the pupils upload their homework, including large video files, have discussions, and receive messages from the teacher about homework. The school has its own intranet, but it is slow, not dynamic enough, and you cannot upload large files. The school has established principles about the usage of social networks such as teachers not being friends with the pupils, and they also discuss web ethics. But they have no discussion about the consequences of exposing the enrolled children's personal data on Facebook.

The debate about these risks of losing control over one's data online and how to perform digital self-defence has – up to now – not been very lively, at least in Northern Europe. Educators play an important role in pushing this discussion. There is nothing wrong about a person's individual choice to share everything about themselves, as long as they know what they are doing and acknowledge the risks their acts entail. To do so as a child or teenager, without informed consent, is a different matter however.

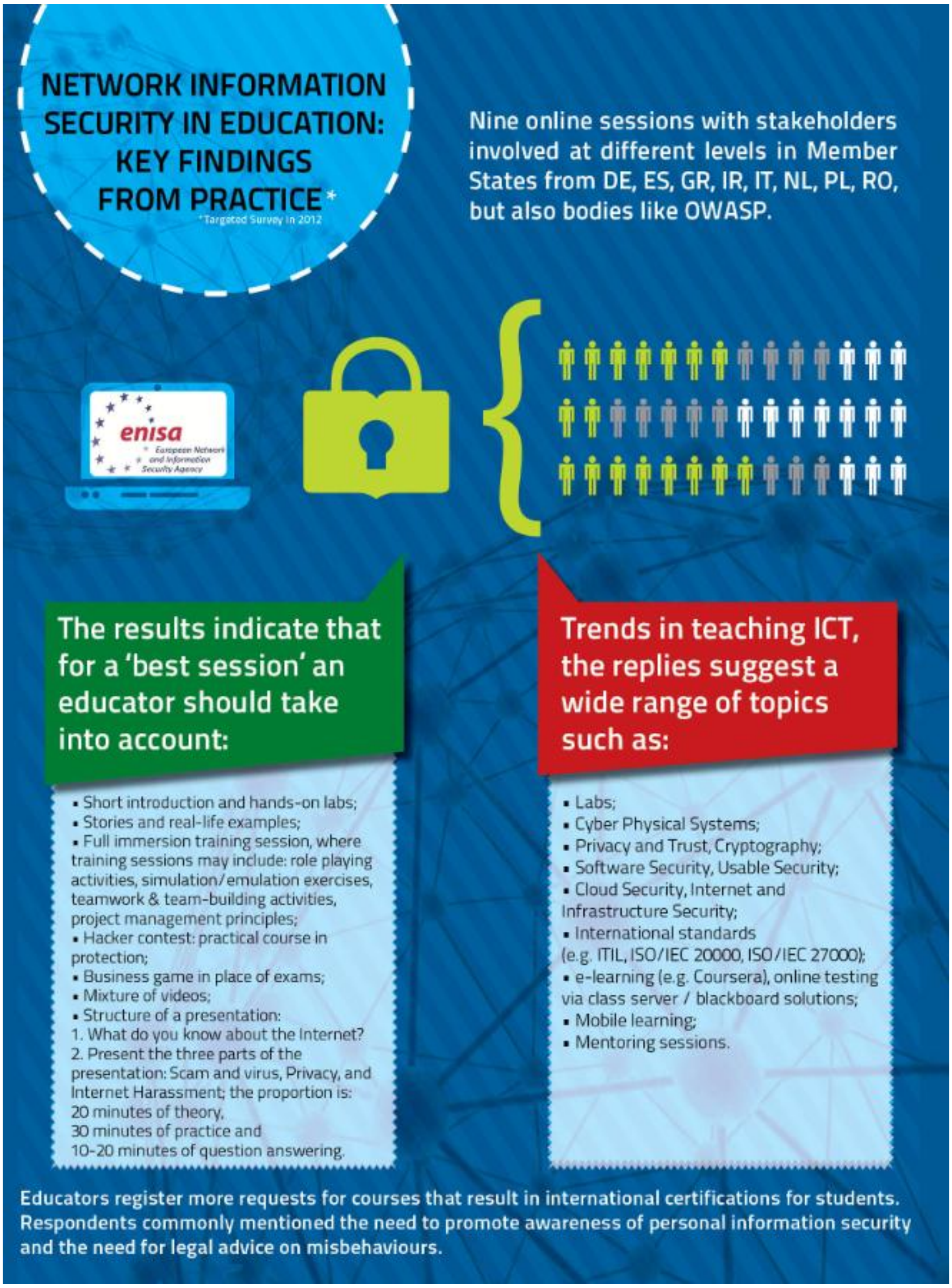
Today, we are polluting our networked world with our personal data, oblivious to the risks for ourselves and our children. Personal data has become the currency that makes the digital economy go round. Our habits, hobbies and hidden secrets have become commoditized, and companies earn billions at our expense when we sign up for and use supposedly 'free' services.

Educators have a special obligation to inform citizens and consumers about the risks of exposing their personal data. Young people need to learn how to keep the pieces of their digital persona to themselves and work with multiple identities. They should 'fake it' online in as many situations as possible when they are not acting professionally.

Faking it online is one great tool to protect your identity in the digital world. It is arguably a rather primitive tool today, but the area of digital self-defense is ripe for innovation and more tools and services to manage multiple identities will soon be launched. Still, using pseudonyms and aliases on the Internet is only a first step. You need to use many other tools, particularly browser extensions to block literally hundreds of companies from tracking you everywhere you go, on the web and with your mobile.

To find out more about the digital footprint and advanced tools see the Electronic Frontier Foundation report 'How Unique Is Your Web Browser?' and ENISA's report 'Study on data collection and storage in the EU'.

4.



NETWORK INFORMATION SECURITY IN EDUCATION: KEY FINDINGS FROM PRACTICE*

*Targeted Survey in 2012

Nine online sessions with stakeholders involved at different levels in Member States from DE, ES, GR, IR, IT, NL, PL, RO, but also bodies like OWASP.

enisa European Network and Information Security Agency

The results indicate that for a 'best session' an educator should take into account:

- Short introduction and hands-on labs;
- Stories and real-life examples;
- Full immersion training session, where training sessions may include: role playing activities, simulation/emulation exercises, teamwork & team-building activities, project management principles;
- Hacker contest: practical course in protection;
- Business game in place of exams;
- Mixture of videos;
- Structure of a presentation:

1. What do you know about the Internet?
2. Present the three parts of the presentation: Scam and virus, Privacy, and Internet Harassment; the proportion is:

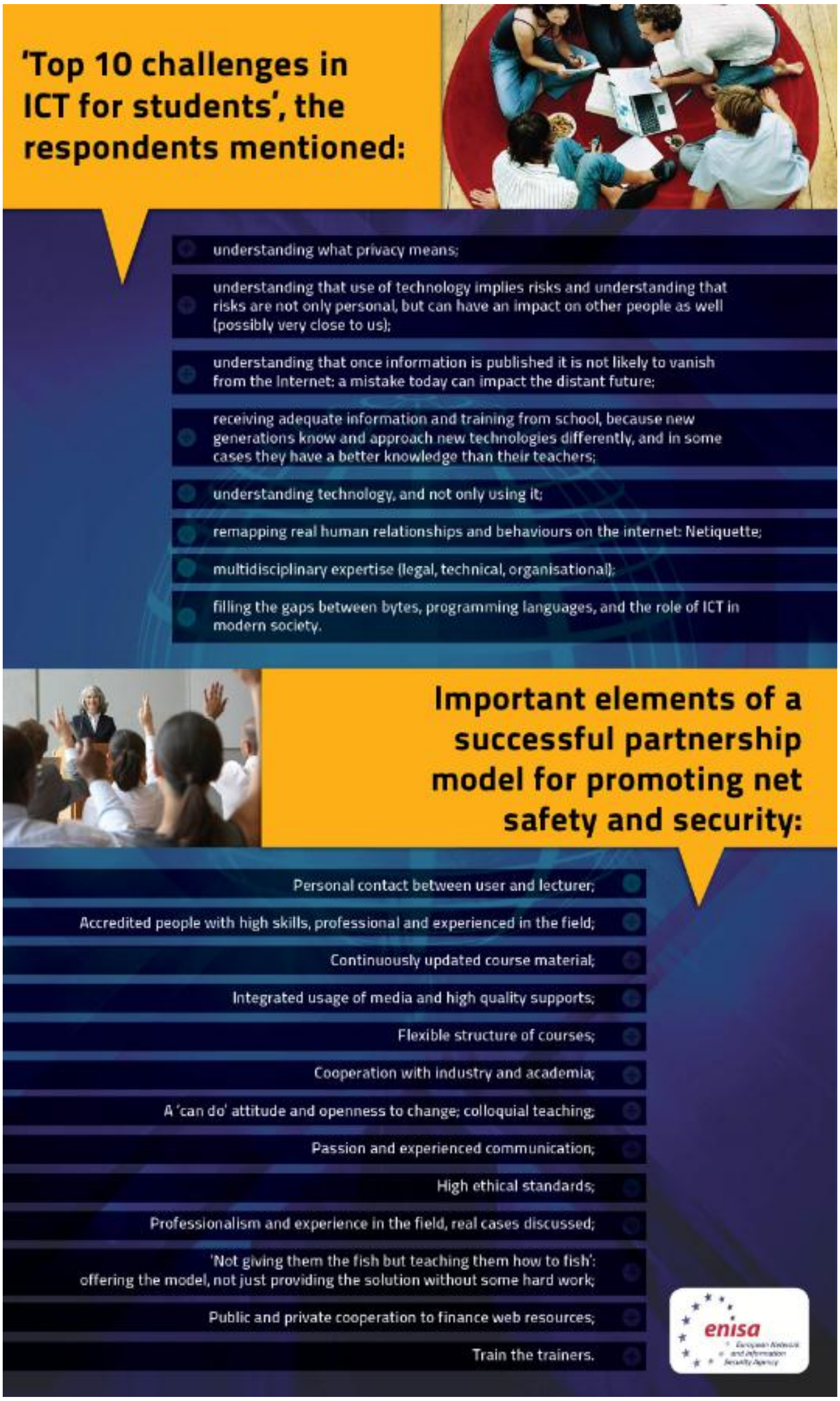
20 minutes of theory,
30 minutes of practice and
10-20 minutes of question answering.

Trends in teaching ICT, the replies suggest a wide range of topics such as:

- Labs;
- Cyber Physical Systems;
- Privacy and Trust, Cryptography;
- Software Security, Usable Security;
- Cloud Security, Internet and Infrastructure Security;
- International standards (e.g. ITIL, ISO/IEC 20000, ISO/IEC 27000);
- e-learning (e.g. Coursera), online testing via class server / blackboard solutions;
- Mobile learning;
- Mentoring sessions.

Educators register more requests for courses that result in international certifications for students. Respondents commonly mentioned the need to promote awareness of personal information security and the need for legal advice on misbehaviours.

5.



'Top 10 challenges in ICT for students', the respondents mentioned:

- understanding what privacy means;
- understanding that use of technology implies risks and understanding that risks are not only personal, but can have an impact on other people as well (possibly very close to us);
- understanding that once information is published it is not likely to vanish from the Internet: a mistake today can impact the distant future;
- receiving adequate information and training from school, because new generations know and approach new technologies differently, and in some cases they have a better knowledge than their teachers;
- understanding technology, and not only using it;
- remapping real human relationships and behaviours on the internet: Netiquette;
- multidisciplinary expertise (legal, technical, organisational);
- filling the gaps between bytes, programming languages, and the role of ICT in modern society.

Important elements of a successful partnership model for promoting net safety and security:

- Personal contact between user and lecturer;
- Accredited people with high skills, professional and experienced in the field;
- Continuously updated course material;
- Integrated usage of media and high quality supports;
- Flexible structure of courses;
- Cooperation with industry and academia;
- A 'can do' attitude and openness to change; colloquial teaching;
- Passion and experienced communication;
- High ethical standards;
- Professionalism and experience in the field, real cases discussed;
- 'Not giving them the fish but teaching them how to fish': offering the model, not just providing the solution without some hard work;
- Public and private cooperation to finance web resources;
- Train the trainers.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu