



Network Information Security in Education

Consolidated ENISA contribution





Acknowledgements

This Report is the outcome of collective effort from between the Ministry of the Economy and Foreign Trade of Luxemburg and ENISA. ENISA would like to thank Mr Francois Thill, Assistant Director for Communications and his team for the open and constructive cooperation that led to this deliverable.

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.

Contact details

For contacting ENISA or for general enquiries on Network Information Security in Education, please use the following details:

Daria Catalui, NIS in Education and Stakeholder Management, Seconded National Expert, ENISA

E-mail: daria.catalui@enisa.europa.eu

Louis Marinos, Senior Expert Risk Analysis & Management, ENISA

E-mail: louis.marinos@enisa.europa.eu

Internet: <http://www.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 ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. 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.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2011

Contents

1	Executive Summary	2
2	Introduction	3
2.1	Target audience	4
3	Related work	5
4	Concise ENISA Material.....	8
4.1	Cyber-bullying and online grooming: helping to protect against the risks	8
4.2	Children on virtual worlds: What parents should know	11
4.3	Awareness Raising Quiz Templates	14
4.4	“Guidelines for Parents, Guardians and Educators” report of ITU in cooperation with ENISA	15
4.5	Security Issues and Recommendations for Online Social Networks	18
4.6	About cookies	20
4.7	Virtual Worlds - Real Money	21
4.8	Secure printing.....	23
5	Conclusions / Recommendations.....	25
6	Annex I: References	26
7	Annex II: Abbreviations.....	28
8	Annex III: Related work.....	29
9	Annex IV: Slides for presentation	30

1 Executive Summary

The Report on Network Information Security (NIS) in Education comes at a time when education and ITC are interrelated and interconnected more than ever. The challenge of the digitally active citizen is to remain informed on the news coming from the dynamic field of ITC and of Information Security in particular.

Long life learning, formal, non-formal and informal education are on the agenda of policymakers. Children, youth and their peers, parents and educators are all part of the discussion and the recommendation is that they should cooperate and get involved as much as possible.

Through Network Information Security in Education we understand the transmission of basic safety information to the young, citizens using the internet.

Our intention with is to start the knowledge transfer process between all involved actors in order to achieve sustainable results with a real impact on the European digital citizen. One way to achieve this is by disseminating the work done in the last few years by ENISA by using a language that can be understood by the target group. We have summarized the findings of ENISA reports by means of concise information in form of fiches. Interested parties can read and use this material and, if necessary, look for further details in the full documents. The selection of the reports was done in order to deliver content that is relevant to can be directly used for educational purposes.

In addition to the fiche produced, within this report we would like to point the excellent work in the field done by a series of organisations (national and international). In order to be updated and use the most relevant information needed we included some recommended readings both under “Related Work” in the Annex (see Annex III: Related work).

In the policy flagship of the European Commission, The Digital Agenda for Europe¹, it is mentioned that “*Youth engagement will make the Digital Agenda a reality*”. The information included in this consolidated report supports the process of being better informed, better educated and better involved in the area of NIS, thus contributing towards the objectives of the Digital Agenda.

¹ <http://blogs.ec.europa.eu/neelie-kroes/youth-engagement-will-make-the-digital-agenda-a-reality/> (accessed 25 October 2011)

2 Introduction

The purpose of this document is to present a consolidated version of available ENISA results in a form that is adequate for use within education. This material targets primary education and especially educators, parents and to some extents teenagers.

The idea was to simplify relevant ENISA deliverables and bring them to a form that will allow easy adaptation to educational objectives, identification of competencies needed and/or direct use through relevant stakeholders. Our aim is not to substitute excellent existing material in this area, but rather to provide concise information from ENISA work that can be easily integrated into existing educational material. The text used in the topics presented below has been extracted from relevant ENISA publications.

The present work was the result of a fruitful cooperation between Ministry of the Economy and Foreign Trade of Luxemburg and ENISA: based on the structure of available educational material of the Member State, existing ENISA material has been digested in order to be used by Member States. After interaction with various players, we have short-listed ENISA deliverables in the following areas:

- Cyber Bullying / online Grooming²
- Children on virtual worlds³
- Awareness raising quiz⁴
- Guidelines of Parents, Guardians, Educators⁵
- Security issues in online social networking⁶
- Cookies⁷
- Security issues in Virtual Worlds and⁸
- Secure printing⁹

The format selected for the presented information consists of:

² <https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/>

³ <http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds>

⁴ <http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-en>

⁵ http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians

⁶ <http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks>

⁷ <http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies>

⁸ <http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming>

⁹ <http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing>

- a short description of the topic/area,
- a reference to main findings/recommendations,
- a reference to the full text and
- a set of slides that can be used for presentation purposes

Our aim is to put interested stakeholders in the position to extract learning objectives from the consolidated information and embed them in their approaches. Due to the assumption that the information of this report will be reused and adapted to particular educational needs and existing methods, we have not spent any effort in layout.

It has to be noted, that the present material is a compilation of relevant ENISA work that has been delivered during the last 3-4 years.

2.1 Target audience

As stated in the WK 2011¹⁰ the Agency supports an open multi-stakeholder dialogue and, for that reason, maintains close relations with industry, the academic sector and users. According to this, this report targets all stakeholder groups who either have stakes or are interested in the issue of NIS and education.

As already mentioned, this report aims at all individuals who are concerned with primary education. This includes parents, guardians and educators, responsible authorities of Member States (e.g. Ministries, national organisations related to education, volunteer organisations, interest groups, etc.). Furthermore, this material can be used by teenagers themselves to become an insight into various NIS issues in the mentioned areas.

¹⁰ <http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011/view>
(accessed 25 October 2011)

3 Related work

In the last years, a series of reports and articles have referenced the issue of NIS in Education. We have chosen to quote some of the sources in order to provide a general overview on existing material in this domain.

EU kids online final report¹¹: talking about the policy implications needed in the field

This is a report issued by EU Kids online. “EU Kids online aims to enhance knowledge of the experiences and practices of European children and parents regarding risky and safer use of the internet and new online technologies, in order to inform the promotion of a safer online environment for children.”¹¹. Main issues addressed are:

- Encouraging children to do more online will improve their digital skill set.
- Teaching safety skills is likely to improve other skills, while teaching instrumental and informational skills will also improve safety skills.
- Inequalities in digital skills persist. So efforts to overcome these are needed.
- Low skills among younger children are a priority for teachers and parents, as ever younger children go online.
- As frequent internet use has become commonplace for many children in Europe, the policy priorities are changed. For children who still lack access, efforts are vital to ensure.
- Digital exclusion does not compound social exclusion. For children with access, efforts are required to ensure their quality and breadth of use is sufficient and fair.
- Efforts to promote children’s digital citizenship – in terms of online safety and good practice – are bearing some fruit, and should be extended.
- Parents are not the only people responsible for children. Teachers also have a vital role to play, and for many children their peers also constitute a valuable resource: 63% of European 9-16 year olds have received internet safety advice from parents, 58 % from teachers and 44% from peers.

¹¹ [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20\(2009-11\)/EUKidsOnlineIIReports/Final%20report.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf) (accessed 25 September 2011)

EC Protecting children in a digital world¹²

This document is a report from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity and of the Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audio-visual and online information services industry. It contains the following reference to education:

- Media literacy and awareness-raising initiatives are partly integrated into formal education and some efforts are also being made to sensitise parents and teachers. However, an assessment carried out by the Commission in 2009 showed that even though the topic is included in national curricula in 23 European countries, actual delivery of such education is fragmented and inconsistent.

ITU research¹³, Targeting youth could be transformational

In a report on ICT pricing and penetration ITU stipulated that information and communication technology (ICT) uptake continues to accelerate worldwide, spurred by a steady fall in the price of telephone and broadband Internet services. Among the comments, the following references to young people have been made:

- The report “Measuring the Information Society 2011” suggests that the main barriers to Internet use are not always related to infrastructure and price. Usage patterns show major differences related to education, gender, income, age and geographical location of users (urban/rural). For example, there is remarkably little difference in patterns of Internet use among highly educated, high-income individuals across the developing and developed worlds. People with higher educational degrees use the Internet more than those with a lower level of education, and in most countries more men than women are online.
- Young people (below the age of 25) are online more than older ones; and there is a higher level of Internet use among those currently in school compared with those no longer studying. Assuming that people will continue using the Internet once they have become accustomed to being online, those currently enrolled at school or university are more likely to be future Internet users. For young people all over the world social networking and user-created content like blogs have become key drivers of Internet uptake.

¹² http://ec.europa.eu/avpolicy/reg/minors/rec/2011_report/index_en.htm (accessed September 2011)

¹³ http://www.itu.int/net/pressoffice/press_releases/2011/31.aspx (accessed 16.09.2011)

- Given that 46% of the population in developing countries is below the age of 25 (representing more than 2.5 billion people), the report suggests that one of the most effective ways to increase Internet use in these countries is by targeting the younger generation – for example through connecting schools and other educational institutions, and improving enrolment rates.

The great schools revolution, The Economist¹⁴

In a report on reforming education, The Economist refers to issues in future education that are indicative for the role of new technologies and kids' skills:

- Technology has also made a difference. After a number of false starts, many people now believe that the internet can make a real difference to educating children. The growing need for workers to keep upgrading and adapting their skills is one of the themes of a new book, "The Shift: The Future of Work is Already Here", by Lynda Gratton of the London Business School. She argues that the pace of change will be so rapid that people may have to acquire a new expertise every few years if they want to be part of the lucrative market for scarce talent. She calls this process "serial mastery" and notes that the current educational system in most countries, from kindergarten through university, does a poor job of equipping people for continuous learning. There is likely to be a wave of innovation in further education, particularly online, that will cater to this need in a more flexible, personalized way than the traditional degree or postgraduate course.
- While there is convergence in the Member States that promoting self-regulatory measures (codes of conduct) is useful, there is persistent concern that the protection levels achieved in this field still differ significantly. Going forward, existing measures against illegal or harmful contents should be constantly monitored in order to ensure their effectiveness. For instance, reporting points for this type of content, provided by the content provider and to be used by children and parents are being developed and supported by functioning back office infrastructures, but all these initiatives lack common features and economies of scale that would increase their efficiency.

¹⁴ http://www.economist.com/node/21529014?fsrc=nlw|edh|09-15-11|editors_highlights (accessed on 17 September 2011)

4 Concise ENISA Material

In the following, we present fiches covering the identified NIS areas that are relevant for educational purposes. Please note that the discussions below are in most cases directly taken from the corresponding ENISA reports. We recommend visiting the ENISA reports in order to obtain detailed material.

4.1 Cyber-bullying and online grooming: helping to protect against the risks

Children are the most valuable part of every society, regardless of culture, religion and national origin. They depend on the care they receive from their parents, the school and their social environment. Duty of care makes parents worry about any of their children's activities that might carry risks, such as extreme sports, or the use of technology. This last topic particularly concerns parents, as they often they do not feel as confident with technology as their children, who:

- Have fun in using technology/gadgets
- Use technology intuitively
- Develop an understanding for usage of technical features very easily
- Become very familiar with innovations
- Use ICT as a learning tool
- Use technology in communicating with their friends

What is Bullying and Grooming?

One definition views bullying in terms of its negative impact on the victim, and sees it as the negative and damaging treatment of another in such a manner that it causes the target to suffer and feel humiliated or vulnerable, and which has a detrimental and stressful effect on him/her. As with harassment, bullying is defined largely by the impact of the behaviour on the recipient, not its intention. Bullying may therefore be seen primarily in terms of aggression, or long-standing violence, physical or psychological, conducted by an individual or a group, and directed against an individual who is not able to defend him/herself in the actual situation.

The purpose of grooming is to make a victim. Grooming is done to choose a victim, to see if the person may cooperate with sexual abuse because of the imbalance of power and coercion. Grooming is done to make a potential victim feel comfortable enough to be close to an offender, to be alone with an offender, and after the ABUSE, to keep the behaviour a secret.

Recommendations

ENISA has issued recommendations to mitigate the risks young people are exposed to in cyber space. The recommendations are divided into groups according to the particular group concerned:

What should parents / guardians / educators do?

- **ENHANCE LEVEL OF BEHAVIOUR KNOWLEDGE:** Enhance skills of parents and educators with regard to knowledge of the online behavioural patterns of minors. Keep continuous communication with parents/educators. Discuss irregularities and consult experts in that area (behavioural psychologists) and participate in knowledge sharing activities relating to that area.
- **ENHANCE KNOWLEDGE ON TECHNOLOGY:** Undertake knowledge transfer to parents/educators with regard to technical issues. Depending on the role in duty of care/education, different levels of knowledge would be necessary.
- **ENHANCE PRIVACY POSTURE:** Teenagers, parents and educators should be kept informed about privacy issues with regard to the cyber world.
- **TRIGGER KNOWLEDGE EXCHANGES:** Technological knowledge should be regularly exchanged between parents and minors. By keeping an open channel with teenagers on technological issues, it is easier to assess their knowledge, level of interest, level of use and usage patterns.
- **USE OF SPECIALISED SECURITY CONTROLS FOR PARENTS/EDUCATORS:** Consider using security controls that are especially customised for use by parents/educators.
- **OFFER SUPPORT FOR TEENAGERS AT SCHOOLS:** It is important to identify potential cyber bullying and online grooming attacks as early as possible. For this reason, teenagers should have immediate access to specialised advice points that are located at schools, to which they can turn in cases where support is required.

What should Teenagers do?

- **USE OF SPECIALISED SECURITY CONTROLS FOR TEENAGERS:** Consider the deployment of security controls for devices used by teenagers in order to prevent easy access to information.
- **ADAPT EXISTING SECURITY CONTROLS TO TEENAGERS:** Currently, in many areas of everyday life, there are security/safety controls that are adapted to children (e.g. cars, planes, ships, toys, etc.). A similar approach should be introduced in cyber space. We

therefore recommend considering the deployment of security controls that are specially customised for use by teenagers/minors

- **DEVELOP ONLINE RATING SCHEMES:** In the TV and film industries, parental guidelines exist in order rate television programmes in terms of explicit sexual content, graphic violence and strong profanity. In the area of computer and video games, similar guidelines exist to score/classify them accordingly. Similarly, the establishment of parental guidelines for online content (services, web sites, social networking applications, etc.) could be considered.
- **PERFORM PRIVACY IMPACT ASSESSMENTS:** Numerous web applications/services process significant amounts of personal data (e.g. social networking sites). It is recommended that criteria should be developed in order to identify application areas where a Privacy Impact Assessment needs to be performed prior to the deployment of the service.
- **DEACTIVATION OF ALL ACTIVE COMPONENTS:** Various handheld devices, portable computers, etc. may have applications installed that have active components, that is, they communicate/process data (e.g. location data, movement data, etc.) in the background. We recommend that users are equipped with functions allowing them to stop any background functions communicating personal data to some service/application providers.
- **ENHANCE AGE ORIENTED ACCESS CONTROL:** We recommend that the age of users becomes an integral part of their credentials throughout the entire infrastructure and in particular the authentication/authorisation mechanisms used.

In order to assess the risks, we used the scenario “Kristie online” details of which can be found in the ENISA report

For more details please visit:

<https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/>

4.2 Children on virtual worlds: What parents should know

With every passing day, a new social-networking website seems to spring up. Online users are spoiled for choice. From Facebook to Bebo, MySpace and Second Life to the business-oriented LinkedIn. But there's a new online phenomenon that's growing and it's for the younger generation. The biggest concerns about virtual worlds are the online safety of children (7 years old and under) and tweens (8-12 years old) and how they can be protected from online predators. Adults must assist children to ensure positive experiences in these three-dimensional environments.

Parents are naturally concerned about how their children are using and acting in the virtual worlds. Information is needed to ensure that parents are able to decide, with their child, what is appropriate and safe for their use, as well as how to behave responsibly in the virtual worlds.

What are virtual worlds?

A virtual world is a computer-based simulated environment intended for users to inhabit and interact via avatars. These avatars are usually depicted as textual, two-dimensional, or three-dimensional graphical representations, although other forms are possible (auditory and touch sensations for example). Some, but not all, virtual worlds allow for multiple users.

The computer accesses a computer-simulated world and presents perceptual stimuli to the user who, in turn, can manipulate elements of the modelled world and thus experiences telepresence to a certain degree. Such modelled worlds may appear similar to the real world or instead depict fantasy worlds. The model world may simulate rules based on the real world or some hybrid fantasy world. Examples of such rules are gravity, topography, locomotion, real-time actions and communication.

Why do children access virtual worlds?

Young people access virtual world sites for a variety of different reasons including the following:

- Interaction with friends in a new environment and in real time, and sharing interests
- Creating and joining communities or interest groups, e.g. music, football etc.
- Communicating thoughts and information on areas of interest through blogs, instant messaging and other tools
- Meeting new people and eventually making new friends
- Creating and sharing original and personal content, such as images, pictures and videos, to expand opportunities for self-expression.
- Creating, publishing and sharing music

- Playing games
- Having their own space, even when parents and carers are present
- Experimenting with their identity, new social spaces and boundaries

Stories and analysis conducted by ENISA have highlighted four main areas of concern:

- Bullying
- Harassment
- Illegal content
- Child abuse

In addition, risks are increased by:

- Unsecure environments
- Lack of educational content
- Product placement in virtual worlds
- Marketing to children
- Cost of engagement:
 - Monthly fees
 - Product purchase
 - Advertising

How can parents and guardians support children?

- Read the terms and conditions of use with their children before they enter the virtual world, discuss safety precautions together, set some basic rules and monitor use to ensure that the rules are respected.
- Educate young users about the responsible use of technology in general, encouraging them to listen to their instincts and use their common sense.
- Ensure use of technical solutions such as:
 - Filters and parental controls.

- User history.
- Confirm the use of automated moderation, such as text filtering which recognises specific words patterns and URLs or more sophisticated filters which include the Anti-Grooming Engines (AGE).
- Ratings: parents and guardians should be aware of rating symbols and their use as an important tool to protect young users from inappropriate services and content.
- Age verification.
- Check that the virtual world is monitored through active in-game and/or silent moderation.
- Stay involved in young users' activities in the virtual world.
- Stay calm and don't jump to conclusions if you hear or see of anything that concerns you about your child's behaviour or the behaviour of one of their online friends. If your children fear that you will simply cut off their social lifeline, they are likely to be increasingly reluctant to share problems or concerns they may have.
- Be open minded to reports from the virtual world community teams that your child may behave quite differently online than offline, face to face with you.
- Learn the online culture so you believe the typical excuses young people give when faced with accountability for their behaviour online, such as —someone stole my account.
- Teach your children not to share their virtual world access passwords with friends or siblings.
- Contact the Community Head via the virtual world's website contact page and share your concerns and questions.
- Don't assume everyone on the net is targeting your child. Statistics show that offline problems with paedophiles far outweigh online incidents. In general, children's sites can be safe and can provide a wonderful, creative social and educational experience for your child but only if you stay involved and aware.

As a consolidation of the above mentioned information, ENISA has issued a poster with 10 internet tips for parents and guardians (see and feel free to use this [poster](#)).

For more details please visit:

<http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds>

4.3 Awareness Raising Quiz Templates

What is the content of the Quiz?

The objective of the developed quizzes is to give the respondent an appreciation of their level of awareness and hopefully serve as a tool to encourage further interest in the values and risks of using computers and utilizing online services on the Internet. Hence they should not be perceived as comprehensive self-tests of individual's current level of awareness and knowledge. Rather, they aim at drawing the attention to the right direction and pinpoint to the topics that are worth elaborating to increase security awareness. Target groups of this ENISA work are parents, end-users and Small Medium Enterprises (SMEs).

This material exists in different languages (EN, ES, DE, FR, IT, DA, PL), making it attractive to a large number of potential users.

Due to the length of the quizzes, we just give below an overview of the parent's quiz, while we propose interested individuals to look at the ENISA report and identify interesting parts (i.e. pages 13-21 of the ENISA report). We expect that identified parts can be directly re-used as they are generic and comprehensive.

Overview of Parents Quiz

In the context of NIS in Education, of particular interest is the part of the quiz related to parents. The aim of this quiz is to provide a means for parent to test their awareness and knowledge on a number of topics concerning child's use of the computer and online services on the Internet. It can serve as a tool to encourage further interest in the values and risks of having your child using the Internet.

The parents quiz covers the areas: PC Usage of Kids, Privacy & Social Networks, Illegal Content, File Sharing and Cyber-Bullying.

For more details please and for end user's quiz, please visit:

<http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-en>

4.4 “Guidelines for Parents, Guardians and Educators” report of ITU in cooperation with ENISA

Understand the type of online experience your kid is looking for

The Internet has great potential as a means of empowering children and young people to help and find things out for themselves. Base learning on emotional experiences, teaching positive and responsible forms of online behaviour is a key objective. In doing so, it is important to understand the type of online experience your kid is likely to look for (see pages 12-13 of the report). This information is an important determinant for the types of risks kids are exposed and consequently the type of protection that will be required.

What many parents, guardians and educators don't know?

Recent analysis conducted by ENISA has highlighted that in most cases parents and guardians are not aware of details concerning the online experiences their children are likely to encounter and the risks and vulnerabilities related to various online activities. Children can be online using different platforms and devices which can include:

- Personal computers
- Mobile phones
- Personal digital assistants (PDAs).

What is the role educators can play?

It is very important that educators do not make any assumptions about what children and young people may or may not know about e-safety issues. There are many misconceptions about the Internet and what either is, or is not appropriate. For example many teenagers share passwords with each other and this is often seen as a sign of true friendship. An important role for educators is to teach children and young people about the importance of passwords, how to keep them safe and how to create a strong password. Similarly, with regard to issues of copyright, many adults are horrified at the apparent lack of concern that younger users have about downloading illegal music and video. Children and young people are hugely lacking in knowledge regarding issues of legality concerning copyrighted content online. Again, there is a clear role for educators to play here in explaining this to pupils. Schools have the opportunity to transform education and help pupils to fulfil both their potential and to raise standards with ICT's. However it is also important that children learn how to be safe when they are using these new technologies, particularly Web 2.0 collaborative technologies such as social networking sites, which are becoming an essential aspect of productive and creative social learning. Educators can help children use technology wisely and safely by:

- Making sure that the school has a set of robust policies and practices and that their effectiveness is reviewed and evaluated on a regular basis.

- Ensuring that everyone is aware of the acceptable use policy and its use. It is important to have an AUP which should be age-appropriate.
- Checking that the school's anti-bullying policy includes references to bullying over the Internet and via mobile phones or other devices and that there are effective sanctions in place for breaching the policy.
- Appointing an e-safety coordinator.
- Making sure that the school network is safe and secure.
- Ensuring that an accredited Internet service provider is used.
- Using a filtering/monitoring product.
- Delivering e-safety education to all children and specifying where, how and when it will be delivered.
- Making sure that all staff (including support staff) has been adequately trained and that their training is updated on a regular basis.
- Having a single point of contact in the school. And being able to collect and record e-safety incidents which will give the school a better picture of any issues or trends which need to be addressed.
- Ensuring that the management team and school governors have an adequate awareness of the issue of e-safety.
- Having a regular audit of all e-safety measures.

What are the elements in a safe ICT Environment?

Creating a safe ICT learning environment has several important elements which include the following:

- responsibilities, policies and procedures
- an effective range of technological tools
- a comprehensive e-safety education
- programme for everyone in the establishment
- a review process which continually monitors the effectiveness of the above

It is, therefore, crucial that parents and educators are able to decide, with their child what is appropriate and safe for their use, as well as how to behave responsibly using ICTs. In working together, parents, educators and children can reap the benefits of ICTs, while at the same time minimizing the possible dangers for children.

For more details please visit:

http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians

4.5 Security Issues and Recommendations for Online Social Networks

What are the vulnerabilities of Social Networks?

Online Social Networks or Social Networking Sites (SNSs) are one of the most remarkable technological phenomena of the 21st century, with several SNSs now among the most visited websites globally.

The impact of cyber-stalking and cyber bullying on the victim is well known and can range from mild intimidation and loss of privacy to serious physical harm and psychological damage. Various factors make SNSs particularly vulnerable to this kind of exploitation:

- Many schools ban the use of SNSs at school, which acts as a strong disincentive to the reporting of bullying.
- The ease of remaining anonymous (using a fake profile).
- The ease of communicating with restricted groups of people (a feature which can be very beneficial if used for the right purposes).
- The one-stop-shop effect. SNS provides all the usual tools and attacks used by a cyber-bully, and more, in a single interface (IM, mobile messaging, fake profiles and slander, etc.) gap. Teachers and adults are frequently unable to intervene because they are not familiar with the technology used.

Forms of cyber-bullying behaviour that can be carried out on SNSs

Various types of activities can be seen as form of cyber-bullying. Early identification of each of these types might lead to an effective surfacing of negative impact to the victims:

- Flaming: Online fights using electronic messages with angry and vulgar language.
- Harassment: For example, repeatedly sending hurtful or cruel and insulting messages; gaining access to another's username and password in order to send inappropriate messages to friends' lists.
- Denigration: Setting up accounts pretending to be people in order to humiliate them; sending or posting gossip or rumours about a person to damage his or her reputation or friendships, e.g., the creation of 'Hate' websites, the posting of jokes, cartoons, gossip and rumours, all directed at a specific victim; posting harmful, untrue and/or cruel statements or pictures, and inviting others to do the same, or to comment on them.
- Impersonation: Pretending to be someone else and sending or posting material to get that person in trouble, put them in danger or to damage their reputation or friendships.

- **Outing:** Sharing someone's secrets or publishing embarrassing information or images online.
- **Trickery:** Talking someone into revealing secrets or embarrassing information, then sharing it online.
- **Exclusion:** Intentionally and cruelly excluding someone from an online group, for example, a group of offline friends deciding to ignore a specific individual as a form of punishment.
- **Stalking:** Typically linked to a problematic intimate relationship, repeated, intense harassment and denigration that includes threats or creates significant fear.
- **Threatening behaviour:** Either direct or indirect.

Discourage the Banning of SNSs in Schools

A growing number of schools are banning or restricting the use of SNSs in schools. It is recommended that schools and education policymakers should carefully consider the consequences of banning SNSs since they act as a disincentive to the reporting of bullying. It also means that teachers and adults are less likely to learn the skills needed to mentor and monitor young people in this area. Finally it also means that a valuable educational resource is lost.

SNSs should be used in a controlled and open way (i.e. not banned or discouraged), with co-ordinated campaigns to educate children, teachers and parents.

It is not the technologies themselves which are responsible for bullying behaviour but the individuals who misuse them. For this reason, education, the modelling of the positive use of technology by peers, teachers and adults and community self-regulation are all key areas in combating cyber-bullying.

For more details please visit:

<http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks>

4.6 About cookies

What are cookies?

Cookies are small information items stored in user's PCs and used widely by online service providers in order to: run their services, capture user preferences (language, layout, credentials, etc.), identification for shopping list purposes, etc. Any Web Site can issue cookies that are stored on user PCs. All the activities related to storing and sending cookies are invisible to the user and are managed by the visited Web Site.

What are the advantages of using cookies?

From a functional perspective, cookies can be used for:

- User identification and authentication (i.e. avoiding re-identification).
- Statistics on visits such as web locations, number of visits, etc.
- Storing preferences and settings.

From a marketing and online advertising perspective, they could be used to:

- Quantify/evaluate the efficiency of ads (i.e. making it possible to determine how many unique users visited a site as a direct response to an ad).
- Profile users and use the profiles to provide targeted advertising (i.e. behavioural targeting).
- Improve management of advertisements (adaptation to user profile, rotation and duplication avoidance).

What are the security concerns?

Main security concerns related to cookies are related to privacy issues of users and to common attacks that are being made on the basis of information found in cookies:

- Collection of private information on user preferences, visited sites, statistics.
- Modify information (e.g. search results).
- Impersonating users leading to malicious logon into accounts (e.g. banking, e-mail, etc.).

For more details please visit:

<http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies>

4.7 Virtual Worlds - Real Money

What is virtual world security about?

Online gaming (and virtual world) fraud is about misuse of user information related to online games. Such fraudulent activities target real money and are based on the increasing use of malicious programs that specifically target online games and virtual worlds; and the emergence of thousands of new programs aimed at stealing online game passwords.

The attackers aim at stealing virtual objects and virtual property and sell them within an existing, emerging grey-market.

What are the top 5 risks in virtual worlds?

The top five risks in the area of virtual worlds are:

Privacy risks: Users may even disclose more personal data because the virtual environment gives a false sense of security. There is also a trend towards behavioural marketing by “eavesdropping” on avatars.

Avatar identity theft and identity fraud: theft of account credentials (username and password). The main motivation is real-money financial gain, but identity fraud can also be used to damage reputation.

Trading and financial attacks – credit card chargebacks: Whenever an in-game purchase is made with an online payment service (e.g. credit card or PayPal), a full refund can be claimed from the payment company (usually within a month). If a chargeback is issued, reversing these transactions is technically and administratively very problematic.

Risks to intellectual property: Original works can be created in-world using official tools provided by the service provider. The actual rights held by the user are often only vaguely defined and may be invalidated by underlying rights. Also, users of virtual worlds often import copyrighted material without the permission of the copyright owner.

Information security related risks for minors: Minors can be exposed to inappropriate content in MMO/VWs either through the circumvention of age verification techniques or the failure of content rating systems. This exposes them to risks such as disclosure of real-world contact data.

Please note that additional risks can be found in the ENISA report.

What are the most important recommendations?

Recommendations made concern all stakeholder groups related to virtual worlds. Important elements from the recommendations made are hints for users to detect compromise of their data. The following is a check-list which could be used:

- Your character is not in the same place as when you logged out.

- Some of your items are missing.
- Your password is incorrect.
- There are new people on your friends list.
- Some of your characters are missing, or there are new characters.
- The last login on the Account Management does not match when you last logged on

You have received an e-mail from the Game Masters with a warning for something that happened when you were not online.

- Your guild members say that they have seen your character online when you were not playing.

The full set of recommendations can be found in the report.

For more details please visit:

<http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming>

4.8 Secure printing

What is secure printing?

Secure printing is any step taken by an organisation to ensure that: printing devices will remain secure; printed or transmitted data will remain confidential, integral and available; the organization will be helped to comply with some of the security standards.

What are the most important recommendations?

1. Define a document flow and management
2. Ensure physical security of printing devices
3. Ensure printing device logical security
4. Ensure security of print data on hard disk or sent-to-printing devices
5. Check how resilient your printing environment is
6. Track printed copied and scanned documents to fax and email
7. Establish a reporting flow on printing jobs
8. Define procedures to govern the use of printing devices
9. Organise awareness training
10. Establish a secure printing strategy
11. Define indicators to measure the success and benefits of the secure printing strategy
12. Establish baseline for evaluation
13. Document lessons learned

Which are the benefits it can bring?

An overview of the many benefits linked to a secure printing environment will help and lead the organization (e.g. school) to better decide about this matter. The following benefits were identified:

- increased security;
- increased flexibility associated with solutions;
- decreased printing costs (e.g. money spent/device; ratio user/device and user/printing);
- reduction of fraud cases;
- increased mobility and flexibility of users, turning what used to be a cost centre to a business enabler;

- achieve compliance (e.g. security audits against standards such as ISO 27002 or PCI DSS);
- enforcement of network central controls;
- full traceability of jobs;
- flexibility in revoking or granting rights to users
- decrease number of incidents reported to IT related to printing issues;
- overall alignment of printing environment with confidentiality, integrity and availability best-practice security model.

Conclusions

Printing devices are handling often confidential information, such as invoices, forms, employee documents and customer data. These devices and the documents they produce remain largely unprotected, leaving as a result business and transaction documents printed susceptible to security breaches. IT asset managers and their organisations should manage print in a proactive way as ensuring a secure printing environment is key for any organization regardless of its size. Security of printing and document capture environments is an integral part of the organization overall security strategy.

For more details please visit:

<http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing>

5 Conclusions / Recommendations

Having in mind that education concerns all of us in our role of student or peer, parent or educator, ENISA invites the reader to stay connected to the safety information coming through all communication channels, use it as much as possible and disseminate it appropriately.

We would like to propose following up ENISA publications, as security issues relevant to education may appear in the coming year. ENISA will try to update this document accordingly by inserting fiches relevant to new related material.

6 Annex I: References

- ENISA. Work Programme 2011 for ENISA, the European Network and Information Security Agency (ENISA website) <http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011/view> (accessed 25 October 2011)
- ENISA and ITU. Guidelines for Parents, Guardians and Educators on Child Online Protection, European Network and Information Security Agency (ENISA website) http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians (accessed September 2011)
- EUKids Online. Final Report EUKids Online including all findings and recommendations [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/EUKidsOnlineIIReports/Final%20report.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf), (accessed 25 September 2011)
- European Commission. 2011 Implementation Report on the Protection of Minors and Human Dignity Recommendations, PROTECTING CHILDREN IN THE DIGITAL WORLD, http://ec.europa.eu/avpolicy/reg/minors/rec/2011_report/index_en.htm (accessed September 2011)
- ITU. Measuring the Information Society 2011 http://www.itu.int/net/pressoffice/press_releases/2011/31.aspx (accessed 16.09.2011)
- The Economist. The great schools revolution, Ed., 17th September 2011, http://www.economist.com/node/21529014?fsrc=nlw|edh|09-15-11|editors_highlights (accessed on 17 September 2011)
- Hogben, Giles, Recommendations for Online Social Networks, European Network and Information Security Agency (ENISA website) <http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks> (accessed August 2011)
- Hogben, Giles, Recommendations for Online Social Networks, European Network and Information Security Agency (ENISA website) <http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks> (accessed August 2011)
- Hogben, Giles, Editor, Online Games and Virtual Worlds, European Network and Information Security Agency (ENISA website)

<http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming> (accessed October 2011)

- Kalmelid, Kjell, Awareness raising quizzes templates: Targeting parents, end-users and SMEs, European Network and Information Security Agency (ENISA website)

<http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-en>, (accessed September 2011)

- Marinos, Louis, Cyber-bullying and online grooming: helping to protect against the risks, European Network and Information Security Agency (ENISA website)

<https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/> (accessed October 2011)

- Santa, Isabella, Children on virtual worlds - What parents should know, European Network and Information Security Agency (ENISA website)

<http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds> (accessed September 2011)

- Santa, Isabella, Secure printing, European Network and Information Security Agency (ENISA website)

<http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing> (accessed October 2011)

- Tirtea, Rodica – ENISA; Castelluccia, Claude – INRIA; Ikonomou, Demosthenes – ENISA, Bittersweet cookies. Some security and privacy considerations, European Network and Information Security Agency (ENISA website)

<http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies>, (accessed October 2011)

7 Annex II: Abbreviations

ENISA European Network and Information Security Agency

EU European Union

ITU International Telecommunication Union

WP Work Programme

MS Member State

NIS Network Information Security

SNS Social Networking Sites

8 Annex III: Related work

Affiliation Name		Link
COE	The internet literacy handbook	http://book.coe.int/EN/ficheouvrage.php?PAGEID=36&lang=EN&produit_aliasid=2023
Eurydice	Key data on ITC and school	http://eacea.ec.europa.eu/education/eurydice/documents/key_data_series/129EN.pdf

9 Annex IV: Slides for presentation



1 Cyber
bullying.pptx

Slides for Cyber Bullying / online Grooming:



2 Children on virtual
worlds - What parent

Slides for Children on virtual worlds:



3 Awareness Raising
Quiz Templates.pptx

Slides for Awareness raising quiz:



4 Guidelines for
Parents, Guardians a

Slides for Guidelines of Parents, Guardians, Educators:



5 Security Issues
and Recommendation

Slides for Security issues in online social networking:



6 Cookies.pptx

Slides for Cookies:



7 Virtual worlds-real
money.pptx

Slides for Security issues in Virtual Worlds:



8 Secure
printing.pptx

Slides for Secure printing:



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