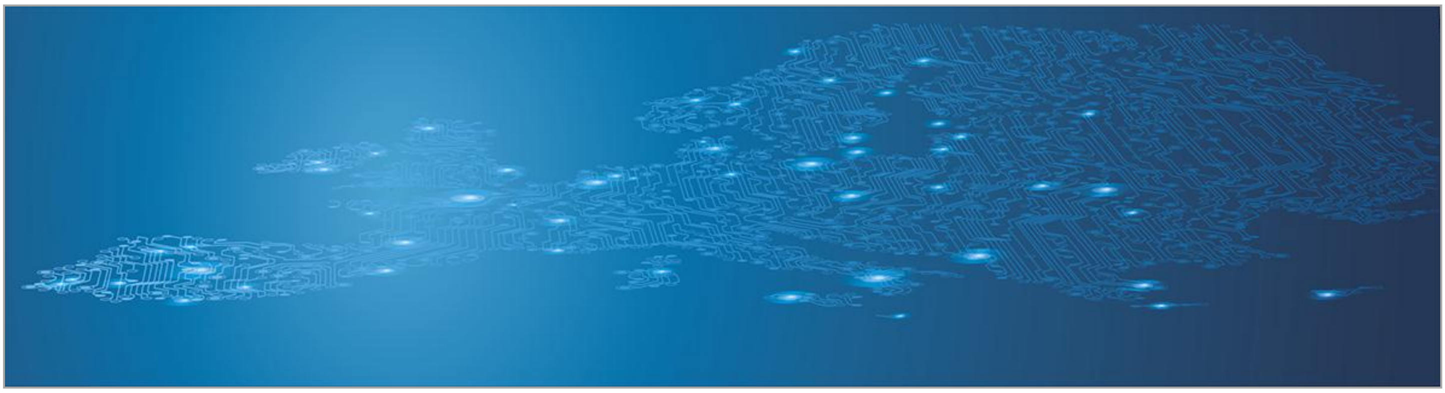


Brokerage model for Network and Information Security in Education

Case studies

2013

European Union Agency for Network and Information Security http://www.enisa.euro

About ENISA

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

Author

For enquiries on EDUCATION refer to Daria CĂTĂLUI, editor of this report, using the following e-mails:

For contacting the editor please use StakeholderRelations@enisa.europa.eu

For media enquires about this report, please use press@enisa.europa.eu

Acknowledgements

We would like to thank the following contributors who joined our effort with valuable insights at country level experience: Sarka Soudkova ([1]), Birgitte Førsund ([2]) and Julia Schaub ([3]).

([1]) Národní centrum bezpečnějšího internet, Prvního pluku 347/12a, Česká republika, (http://www.saferinternet.cz) (http://www.bezpecne-online.cz).

([2]) Birgitte Førsund, Norwegian Centre for information Security (http://www.norsis.no).

([3]) Bundesamt für Sicherheit in der Informationstechnik (http://www.bsi.bund.de) (http://www.bsi-fuer-buerger.de).

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 Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

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

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

Copyright Notice

ISBN 978-92-9204-080-2 doi: 10.2824/29145

Executive summary

By publishing the *Brokerage model for Network & Information Security (NIS) in Education* report, we aim to provide content and promote digital education on network and information security at all levels. The target group is composed of educators such as trainers, teachers and peers involved in formal education and non-formal education, including lifelong learning.In our current brokerage effort we try to connect the nodes in the best way possible by presenting three case studies with countries perspective, from the Czech Safer Internet Centre (NCBI), 'Strategy of community education in project — Prague safe online', from German partners, the Federal Office for Information Security (BSI), '10th anniversary of the Safer Internet Day provides an opportunity to increase awareness', and from Norwegian partners, 'Norwegian Centre for Information Security'. Furthermore we open a discussion about hacking. 'Hacking for good or for bad' is a case study to advance the use of appropriate terms by the NIS in Education community, taking into account the particularity of the given ecosystem. In order to raise awareness of our target group we share the view that everybody should take part in the discussion and share the responsibility of a secure global digital community. As recommendations to be taken into account by NIS in Education stakeholders from Member States we mention:

- Learning experiences on hacking should be organized with a clear focus on educational purpose vs legal implications of misbehaviour;
- Hacker contests and Cyber Challenges should be focusing on protection and receiving tips on preventive actions;
- The community education model should be given further considerations;
- Emphasize on the importance of awareness-raising measures as a continuos cooperation at both national and international levels;
- Relying on more interdisciplinary solutions.

Regarding the general procees we draw the attention on the following recommendations:

1. ENISA and EC should address Cyber Security awareness at all levels in different arenas for sharing information.

2. Awareness organisations should pursue Public-Private partnerships in their Educational attempts towards the digital users.

3. NIS in Education community members should target specific stakeholders with different methods and specific content

The brokerage model for education is thus in focus in the three case studies and we are interested in consulting more partners in the future to identify their brokerage model.

Essential questions: What content in particular should we share? Which stakeholders do we involve? What are the methods that we deploy?

Contents

1. Introduction

The *Brokerage model for Network and Information Security in Education* report is a continuation of *Collaborative solutions for network information security in education* ([4]) (2012), and *Network information security in education: consolidated ENISA contribution* ([5]) (2011). In 2012, we argued that brokerage of information is at the root of the learning cycle and we provided details to justify this by using practical examples from Austria, Denmark and Luxembourg. Our main recommendations were that we should all learn from our peers' best practices and share our own experiences. We also recommended that a 'can do attitude' should be deployed both by educators and by their students of different age groups.

We started with digital education work at ENISA and in this spirit we have been working, throughout 2013, in order to gather evidence on the newest developments and to share ideas among NIS communities.

Furthermore, our main goal in publishing this report was to provide material to the target group and promote digital education on network information security.

The main target group of our report is the same as in previous years. It consists of educators such as trainers, teachers and 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!

We consider cyber security as an enabler and not as a burden, and by concentrating on education we want to emphasise the need to bring the various competences and capabilities of the EU Member States up to speed. Our main goals are to achieve 'Cyber hygiene', 'Netiquette' and being a 'good digital citizen' by involving the users through our partners and specialized communities.

In our current brokerage effort we try to connect the nodes in the best way possible and as a result we present three case studies with countries perspectives, from Czech partners, 'Strategy of community education in project —Prague safe online', from German partners, '10th anniversary of the Safer Internet Day provides an opportunity to increase awareness', and from Norwegian partners, 'Norwegian Centre for Information Security'. The brokerage model for education is in the spotlight in the three case studies and we are interested in consulting more partners in the future regarding their brokerage model.

[4] ENISA Report (2012), https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/collaborative-solutions-for-network-information-security-in-education

[5] ENISA Report (2011), https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/nis-in-education

1.1 Case study: Hacking for good or for bad ([6])

Background

Following up on previous recommendations and trying to monitor their implementations makes an important part of ENISA's work. As mentioned in current and previous education work our main goals are to achieve 'Cyber hygiene' or 'Netiquette' by involving the users through our partners and specialized communities like this one of educators. In June 2012, 45 EU and US representatives from the private and public sectors gathered in Brussels to discuss the topic of involving Intermediaries in Cyber Security awareness, summarized in an ENISA report[7]. In that event Dr. Timmers the EC CONNECT's keynote speaker set the challenge to find ways to make hacking better understood and more suitable as use. It was mentioned that awareness effort may concentrate on 'finding ways to make hacking uncool'. We follow up with a case study on the current use of the term, because we believe that the education practitioners and all other partners in awareness raising should have a clear and common understanding of the term and a unified message to transmit.

How many times a week do you read an article on cyber security and hacking? Although both are popular buzz words and powerful hash tags on social networks, they are also of paramount importance in our daily life at work or during our spare time. In order to raise awareness we are of the opinion that everybody should be part of the discussion and share the responsibility of a secure global digital community. We therefore want to develop on a few considerations about hacking. 'Hacking for good or for bad' is an attempt to advance the use of appropriate terms by the NIS in Education community, taking into account the particularity of the given ecosystem.

The network and information security world uses technical terms on a daily basis and we might easily get caught in discussions about 'botnets', 'bullying', 'spamming', 'identity theft', 'denial of

([6])Many ENISA colleagues contributed with opinions in a thematic discussion and we thank them all; also Annex A contains direct links to thematic materials.

([7]) Involving Intermediaries in Cyber-security Awareness Raising http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/eu-u.s.-event-on-intermediaries-in-cybersecurity-awareness-raising/involving-intermediaries-in-cyber-security-awareness-raising service', 'malware' and 'grooming' and find ourselves using the same term for opposite meanings. Not always do experts or outsiders agree on the definition of these terms – and often terms start to live a life of their own. A good example is hacking. Do we use hacking for good or for bad? What do you think?

Objective

Following the whole debate and reading publications of various actors, we observed that the controversy about the term 'hacking' is still very much alive. It is not a new debate and we do not think that it will end soon as the term is evolving. However, we felt the need to participate with a short summary of the current status. It will represent a common ground for the NIS education community to further transmit a common message to European users. The purpose of the trial is to emphasize on the contextual meaning of the term 'hacking'.

Considerations to take into account

Hacking is what hackers do with the high skills and knowledge they possess. However, the term can have different meanings depending on the context in which it is used. In ENISA's education reports we advocate for good cyber security education in the EU, mentioning labs and hands on experience. Furthermore, we promote the saying 'do not learn to hack, but hack to learn' ([8]).

The shared opinion is that hacking is a neutral term, and that the discussion about ethical-'good hacking' and unethical- 'bad hacking' has to be put into context. For example, hacking is 'uncool' when it is done with malicious intent and hacking is 'cool' when it is done with good intent ([9]). Hacking is neither good nor bad. 'Cracking' would be a better term to use when speaking about bad hacking.

However, it is primarily a mind-set: a way of thinking about security. Its main focus is on attacking systems, but at the same time it is also invaluable for defending those same systems. Because computer systems are very complex, defending them often requires experts to think like attackers. Admittedly, there is a big difference between thinking like an attacker and acting unlawfully; and also between researching vulnerabilities in fielded systems and exploiting those vulnerabilities for personal gain.

The terms hackers and hacking should be used, taking into consideration the context, the background and the community behind it.

Hackers have been around in our society for a long time. Hackers are sometimes described as curious, analytical, innovation-oriented and open-minded experts. However, the sword is double-edged, in the same way that a locksmith's skills is used to help people, but his expertise could also be used to break into somebody's home. Such skills, which can be used to cause great harm, create fear and suspicion in people. However they can also be of great educational value. People are all different. For some it is educational and interesting to see how computers and applications work in depth, whilst others make a living by finding vulnerabilities in computer software and hardware and selling them to people who are willing to pay for the ability to easily break into computers.

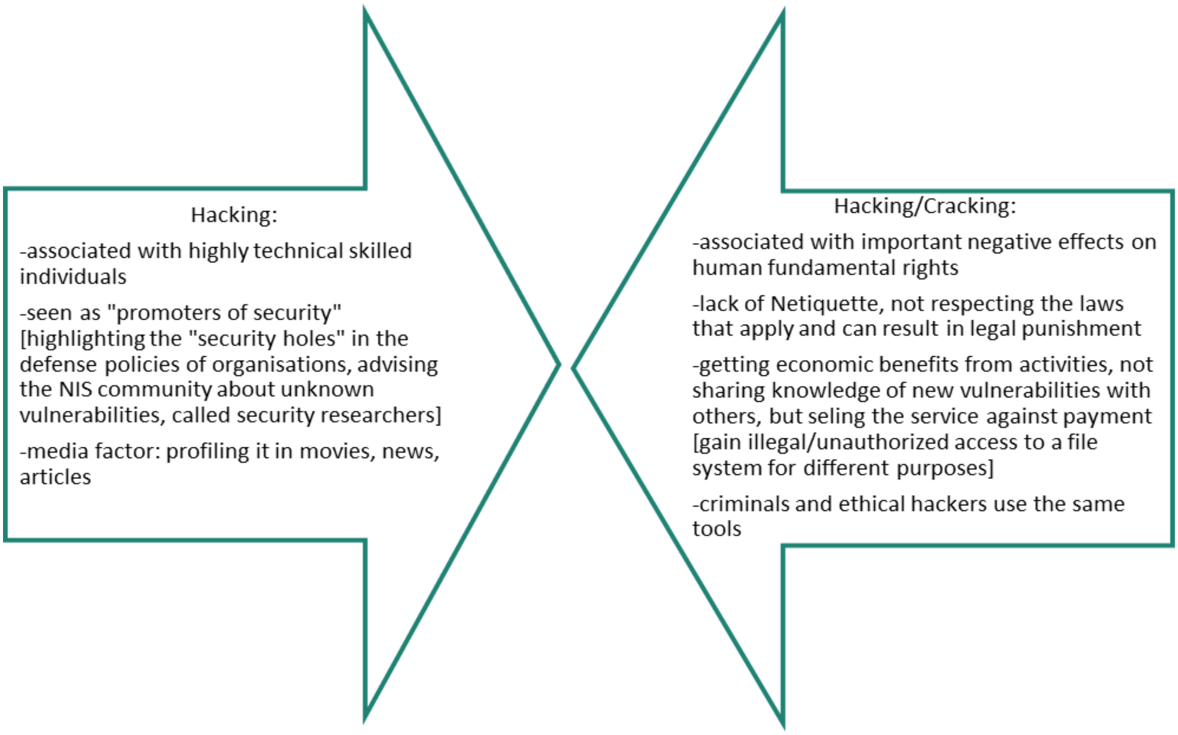
([8]) Darknet's motto
([9]) Reference to MEP Marietje Schaake speeches.

Next steps

In order to clearly set the objective on the learning experience and fill the gaps between the roles of ethical and unethical hacking in society, we recommend the following for a better use of the term:

- Labs, classes and trainings on hacking should be organized with a clear focus on understanding the educational purpose vs. legal implications of misbehaviour;
- Hacker contests and Cyber Challenges should be focusing on protection and receiving tips on preventive actions.

As a conclusion for good cyber security in the EU, MSs should better integrate NIS in public policies in education meant to enhance the technical skills of users and the general understanding of concepts. A summary with remarks is depicted in the graph below:



Hacking:

-associated with highly technical skilled individuals

-seen as "promoters of security" [highlighting the "security holes" in the defense policies of organisations, advising the NIS community about unknown vulnerabilities, called security researchers]

-media factor: profiling it in movies, news, articles

Hacking/Cracking:

-associated with important negative effects on human fundamental rights

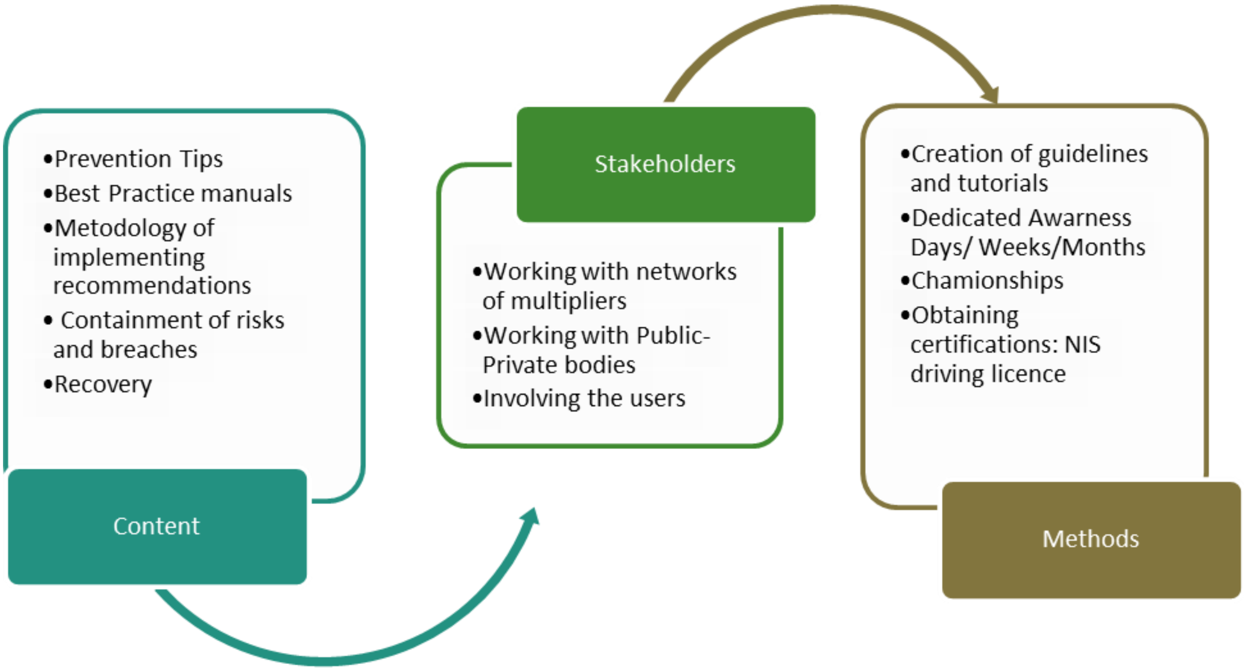
-lack of Netiquette, not respecting the laws that apply and can result in legal punishment

-getting economic benefits from activities, not sharing knowledge of new vulnerabilities with others, but seling the service against payment [gain illegal/unauthorized access to a file system for different purposes]

-criminals and ethical hackers use the same tools

2. Case studies at country level experience

In this chapter we describe experiences at country level, in the Czech Republic, Germany and Norway. We are looking for a brokerage model for network and information security in education that could be shared across European countries to actively educate the digital citizen.


•Prevention Tips
•Best Practice manuals
•Metodology of implementing recommendations
• Containment of risks and breaches
•Recovery
Content
Stakeholders
•Working with networks of multipliers
•Working with Public-Private bodies
•Involving the users
•Creation of guidelines and tutorials
•Dedicated Awarness Days/ Weeks/Months
•Chamionships
•Obtaining certifications: NIS driving licence
Methods

The EU cyber security 'An open, safe and secure cyberspace' strategy ([10]) mentions the development of a roadmap for a 'network and information security driving licence' as a voluntary certification programme to promote enhanced skills and IT competence and other techniques for user empowerment such as cyber security championships, 'Capture the flag' competitions, the 'European Cyber Security Month' advocacy campaign, aligned with other global efforts. Additionally, the strategy calls to '**step up national efforts on NIS education and training'** ([11]), by introducing training on NIS in schools by 2014, training on NIS and secure software development and personal data protection for computer science students, and NIS basic training for staff working in public administrations. ENISA has started the consultation process in order to involve the relevant stakeholders and guide the process for quality results during the next years. We are also keen to search for best practices at country level and pick up the practice to be scaled up to regional, European and international levels.

Promote cyber security awareness at all levels!

([10]) http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 (accessed in October 2013).

([11]) As recommended in the ENISA report, (2012), *Collaborative solutions for network information security in education*.

2.1. The Czech Republic: strategy of community education in the ‘Praha bezpecne online‘/‘Prague safe online’ project ([12])

Background

The Národní centrum bezpecnejsiho internetu/Czech Safer Internet Centre (NCBI) is a non-governmental, non-profit-making working association established to carry out the tasks related to knowledge-building, education and exchange of best practice in the field of safer use of the Internet and new media. It carries out various awareness-raising activities focused on children, their parents and teachers, and strives to engage Czech stakeholders in the promotion of safer use of the Internet.

Objective

The main objective of educational project ‘Praha bezpecne online‘/‘Prague safe online’ is the social protection, especially of children and young people, from the risky phenomena arising online and thus preventing online crime targeting children or committed by the youth themselves. The project raises awareness about safer use of the Internet and new media, and reduces the risk factors of online delinquency. The most important risk factors were determined as:

- minimum knowledge of elementary school pupils and high schools students about the risks of online communication and online-delinquency;
- high level of technical knowledge of pupils and students concerning information and communication technologies;
- high accessibility of information and communication devices;
- immature personal, social and moral competences of young Internet users ;
- Low awareness of the legal consequences of some acts performed online (criminal consequences of some patterns of online behaviour, protection of personal rights and copyrights by the criminal code, etc.);
- low (or zero) awareness of educators and prevention school specialists of online risks and online delinquency;
- Low (or zero) knowledge of information and communication technology teachers, especially about Internet services (social networks, instant messengers, etc.);
- absence of education on the safe and ethical use of the Internet and new media in the elementary and high school curricula;
- low awareness of the public, especially parents, about the online risks and delinquency connected to the use of the Internet and the possibilities of children and youth protection;
- Limited time parents spent with their children.

[12] Contributor Sarka Soudkova, Národní centrum bezpečnějšího internet (http://www.saferinternet.cz).

Method

In the Czech experience-based approach they work on the assumption that prevention efforts focusing on one target group are, by far, not as efficient as if they cover the local community surrounding this target group as a whole. This is the main idea behind the community education, which focuses on the maximum number of specialists who can solve crisis situations connected with the online behaviour of pupils. By linking up these specialists, a ‘safety net’ that can efficiently operate at the local basis, is created. In the same time frame, they work with the parents of the pupils of all the local elementary schools, and of course also with the children themselves.

The following groups were involved in the project:

— Elementary school children;

— parents;

— Educators (teachers, headmasters, school prevention specialists);

— Specialists working with children (social workers, pedagogical-psychological counseling workers);

— The municipality’s prevention specialists;

— police officers from the area (mostly prevention specialists working with schools), probation and mediation service specialists.

Working with all the above-mentioned groups in the same time frame increases the motivation and interest about the topics of the particular groups. In a relatively short period of time, online safety literacy increases in the local community. All the groups involved start communicating with one another, share their newly gained knowledge and experience, and recommend further activities. Schools gain concrete partners for solving problematic situations from the municipality, the police, pedagogical-psychological counseling services; parents, one of the least easily accessible groups, become aware of the extent of the problem and their motivation to actively participate increases.

To target the widest public, the project is accompanied by public awareness campaigns:

— PR in conventional media (articles in newspapers, TV shots, reports from the events, interviews mostly on local TV, radio broadcasting, etc.);

— Outdoor campaigns (posters, city light screens);

— Internet (http://www.saferinternet.cz) websites and websites of cooperating institutions (municipality, Ministry of the Interior, information stalls in schools and other institutions);

— Indoor campaigns (using school facilities, offices of cooperating institutions, etc.).

Every session of the project ends with a national conference. The audience consists of professionals from the groups mentioned above, and of an interested public. These events also attract the media and stakeholders.

Results

The 'Praha bezpecne online'/'Prague safe online' educational project is one of the successful and dynamic developing NCBI projects. In 2011, the pilot of the project started raising the awareness of all the competent people of the selected Prague districts, the municipality prevention officers, school representatives, social workers and police officers. The model gave very good results. This is why, in 2012, the project, focusing on other Prague districts were run on the basis of community education. In 2013 the project is still running in Prague with increased number of participants and the same model is also used for the other regions of the Czech Republic.

The Czech community education model has proved to be an efficient way of involving all the groups dealing with children and young people at risk of online communication. The participants' feedback was very positive, evaluating the activities as very useful and professional.

Next steps

The NCBI will also pursue its community model of education focusing on the awareness raising and prevention of online delinquency and crime committed against and by children and young people in other localities of the Czech Republic.

Impact of Prague safer online project in 2013:

ACTIVITY	Number of seminars	IMPACT
One day workshops for social workers	**12**	**120 social workers**
One day workshop for police officers	**2**	**50 police officers**
One day workshop for prevention specialists	**13**	**120 prevention specialists**
One evening seminars for parents	**30**	**600 parents**
Primary prevention seminars for children	**170**	**4 250 pupils**
Total	**227 events**	**5 140 people**

2.2. Germany: the 10th anniversary of the Safer Internet Day provides an opportunity to increase awareness ([13])

Background

The Federal Office for Information Security (BSI) is responsible for raising the awareness of German citizens in the various subjects of Internet and IT security. The BSI provides practical guidance on the secure handling of electronic communication media. To this end, a series of measures to raise public awareness are implemented continuously, e.g. regular press activities, events like trade fairs or open days, material such as brochures and posters, the citizens' online portal (http://www.bsi-fuer-buerger.de) and the citizen CERT newsletter providing information on general developments and warnings in case of security incidents and security gaps. Furthermore, since 2010, the BSI runs a service centre as point of contact for citizens, on all questions regarding IT and Internet security issues. It offers independent advice and guidance to private users. The service centre is available via phone and email from Monday to Friday between 8 am and 6 pm. In case of enquiries beyond the so-called first level, the BSI's various technical departments are called upon to assist in answering citizens' questions.

In addition to these regular activities, the BSI also makes use of further suitable opportunities to raise public awareness of IT security, one of these being the 10th anniversary of the Safer Internet Day, on 5 February 2013.

Definition of subjects for concrete assistance

In order to provide direct access to private users as a target group and to offer simple and viable solutions, the activities focused on two main topics:

1. Secure mobile use of the Internet;
2. Strong passwords to increase security.

The PR activities started with a radio feature on mobile Internet. The aim was to make private users aware that their mobile devices are small computers which need to be protected against unauthorised access. Another aim was to create awareness that — due to their capability of providing Internet access — smartphones have the same protection requirements as the PC at home. A description of the risks was linked to associated information on security.

[13] Julia Schaub, Bundesamt für Sicherheit in der Informationstechnik (http://www.bsi.bund.de) (http://www.bsi-fuer-buerger.de).

The programme focused, on the following advice:

1. Do not leave the device unattended
2. Enable all existing locking mechanisms such as PIN and display lock
3. Avoid entering sensitive data using public networks
4. Install apps only from trusted sources and check the rights granted to the application
5. Install all available software updates on your device.

To reach a wide audience, the topic was tackled with the help of a broadcast service provider. In addition to the inclusion of an expert interview with previously defined questions, an independent ready-to-broadcast programme was produced. Both elements, radio programme and interview, were offered in the German-speaking broadcast area in the week prior to and on the Safer Internet Day on 5 February 2013, and aired around 40 times around the anniversary date. The programmes thus reached an audience of nearly 4 million radio listeners.

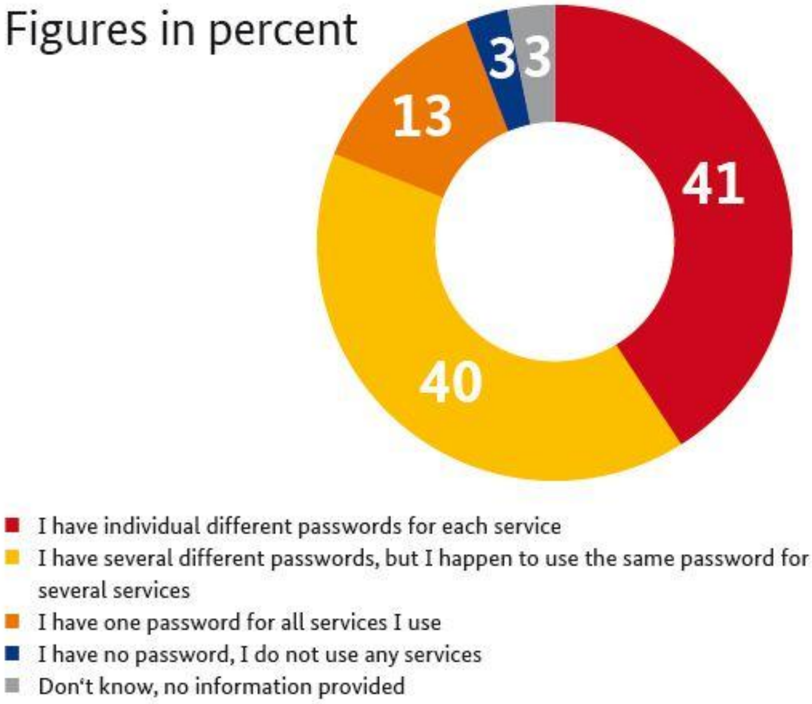
Strong passwords and strong partners

To increase the awareness of password security, the BSI decided to cooperate with a strong partner. The Police Crime Prevention of the Federal States and the Federal Government (ProPK) supported the concept and implementation of the activities. A representative survey[14] among German Internet users was conducted by the market research institute, TNS Emnid, in order to obtain up-to-date and reliable figures regarding the use of passwords by German Internet users.

Password security among German Internet users

The results of the survey allowed some interesting conclusions regarding the way in which the respondents use their passwords. In order to keep the message on how to generate a secure password short, the presentation focused on a particularly distinctive fact: the survey showed that more than half of the Internet users questioned do not assign an individual password for each online service they use.

[14] TNS Emnid BSI



Basis: 1,163 people questioned
Rounding differences possible
Source: TNS Emnid/Federal Office for Information Security (BSI)

This fact was used as a message and paired with the most important advice on secure password generation. While the BSI focused on technical assistance, their cooperation partner, ProPK, outlined the potential consequences under criminal law. These two perspectives ideally complemented each other to highlight the importance of a well-chosen password. The message was published via the various communication channels of the BSI and ProPK on 29 January 2013, one week before the Safer Internet Day. In addition, the topic was featured in a prominent place and complemented by additional information and further references on the BSI's citizens' portal (http://www.bsi-fuer-buerger.de) and the website of ProPK.

Multipliers increase public awareness

As well as the BSI's and ProPK's various newsletters, the message was also sent to different multiplier groups and journalists. This generated further synergy effects such as subject-related interview requests by radio stations. Furthermore, BSI successfully addressed women on IT security matters in the online environment via women-specific media.

The BSI used the International Safer Internet Day to place a number of important IT security topics attracting media coverage. Thanks to the support of cooperation partner ProPK, it was possible to address important target groups beyond the BSI channels to make them aware of the relevance of IT security. The qualitative and quantitative responses to the implemented measures prove that continuous cooperation at a national and international level is an important component of awareness-raising measures for private users on IT security.

2.3. Norway: Norwegian Centre for Information Security [15]

Background

The Norwegian Centre for Information Security (NorSIS) is part of Norway's focus on information security. Their aim is to make information security a natural part of everyone's daily life.
The primary target groups are small and medium-sized enterprises as well as public authorities. They also try to accommodate requests from the public. Their ambition is to provide services for every part of the society. NorSIS will try to reach its objectives through:

- raising awareness about information security through training and information;
- the compilation and creation of guidelines and tutorials concerning information security topics;
- Establishing an overall awareness towards information security.

NorSIS has over 10 years of experience and has nine employees. NorSIS reports to the Ministry of Justice [16] and public security.

Our tools to do our job

To reach out with the message, they need to structure their communication and actions through the media. They have a very good relationship with the Norwegian press, and are also often contacted by journalists as experts in matters concerning 'information security', trends and threat reports. Since NorSIS is an independent organisation, their voice and guiding are valued by journalists from all types of media (daily press/finance).
They also present new research to the media, together with the public and the private sector.

'Arena that they created'

Since they are asked to assist both the public and private sector, they work hard to create different arenas for sharing information and knowledge about information security. For instance:

- organise presentations when requested for businesses, the public or schools;
- arrange about 15 different conferences each year — some are specific adjusted to different branches as oil, energy/power industry, maritime and public sector;
- Arrange 'Security top meetings' that are for invited guests only and limited to about 40 participants from the public and the private sector. This meeting is based on the 'Chatham's rules' and a report is made afterwards for participants only;
- also communicate through four different webpages:
  1. http://www.norsis.no (about organisation, what they do, information, updates and how they work),
  2. http://www.sikkert.no (about National Security Month),
  3. http://www.slettmeg.no (about help to delete info/pictures/films),

[15] Birgitte Førsund, Norwegian Centre for Information Security (http://www.norsis.no).
[16] http://www.regjeringen.no/en/dep/jd.html?id=463

4. http://www.idtyveri.info (about ID theft),

- use social media such as Facebook and twitter;
- educational movies and advertising films are also launched (http:www.youtube.com);
- Work together with all kinds of businesses in Norway to promote awareness about information security. This work is made possible through the sponsor of the program which invites businesses to join the work. The sponsor program for National Security Month is the most popular and they had more than 20 sponsors this year.

Examples of what they do and how

1. Internet voting/2013

The government conducted another pilot of Internet voting for the parliamentary election of 2013, due to the positive experience from the pilot scheme in 2011. The Ministry of Local Government and Regional Development therefore contacted NorSIS. Their job in this matter is to arrange courses in each of the 12 municipalities which were chosen for this pilot scheme. NorSIS developed courses based on guiding from the ministry. This means teaching voters to be 'digital election observers'. Recruiting volunteer observers was done together with the municipalities. They used the local press to get publicity and the municipalities' webpages and social media. In August 2013, NorSIS advisors travelled around Norway to teach voters how to be 'digital election observers' ([17]). If anyone experiences anything wrong, they can report to the helpdesk at the ministry.

2. National Security Month/October 2013

NorSIS is responsible for 'National Security Month' based on an initiative from ENISA ([18]).
This is the third year they organise the National Security Month in Norway and interest in the event has grown — from the government, press, businesses, sponsors and people in general. This year they already have more sponsors than last year, as for instance, the National Cyber Force and Norman (http://www.norman.com). More information can be found, but only in Norwegian (http://www.sikkert.no). They also aimed to sell training packages for employees about information security to businesses all over the country, and work hard to get media coverage. They arranged a press conference and a kick-off event. In October, they shared speeches/communications from voluntary security experts for businesses in Norway.

3. Slettmeg.no (translated to 'delete me')

'Slettmeg' ([19]) is a service from the Norwegian Centre for Information Security (NorSIS). The purpose of this service is to help people who experience privacy violations online. The service was launched in March 2010. It is often referred to in the media and young people in particular need this service — for instance when it comes to Facebook pictures, bullying, or other offensive things.

([17]) For more information: http://www.regjeringen.no/en/dep/krd/press/press-releases/2012/new-pilot-with-internet-voting-in-2013.html?id=710138

([18]) http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-2013-get-involved

([19]) http://www.slettmeg.no/English

Summary

In Norway, NorSIS has established itself as a 'voice of authority' with more than 10 years of experience in promoting awareness about information security. As an independent organisation, they continue to create arenas for sharing, education and increased awareness about information security. The National Security Month has been important for them to create a stronger public–private partnership and to get public attention about a topic that affects us all. Their role as 'coordinator' and 'facilitator' in the security branch in Norway has been even more important lately, since they are now, and will in the future be, relaying on more interdisciplinary solutions to handle cybercrime.

3. Conclusion

The *Brokerage model for Network and Information security in Education* report provides content and promotes digital education on network and information security at all levels. In an attempt to draw the conclusions we would like to mention the following:

- ➢ The terms hackers and hacking should be used taking into consideration the context, the background and the community behind it;
- ➢ From the Czech example we found out that online safety literacy increased in local communities by involving all competent groups and encouraging them to start communicating with each other, share their newly gained knowledge and experience, and recommend further activities. The community education model proved to be an efficient way to involve all the groups dealing with the risks of online communication. The Czech Safer Internet Centre (NCBI) is going to use the model in other regions too.
- ➢ From the German example, we note that Safer Internet Day may be used for a larger purpose, to raise awareness and attract media coverage. With the support of cooperation partner, ProPK, it was possible to address important target groups beyond the BSI channels to make them aware of the relevance of IT security. The qualitative and quantitative responses to the implemented measures prove that continuous cooperation at a national and international level is an important component of awareness-raising measures for private users on IT security.
- ➢ From the Norwegian example we learn the importance of creating different arenas for sharing information and knowledge about information security. NorSIS, established as a ‘voice of authority’, continues to generate arenas for sharing and for education. The National Security Month has been important to build a stronger public–private partnership and to get public attention. In future, they will be relying on more interdisciplinary solutions.

With these examples we have seen different brokerage models for network and information security in education that can be shared across European countries to actively educate the ‘digital citizens’. As recommendations to be taken into account by NIS in Education stakeholders from Member States we mention:

- Learning experiences on hacking should be organized with a clear focus on educational purpose vs. legal implications of misbehaviour;

- Hacker contests and Cyber Challenges should be focusing on protection and receiving tips on preventive actions;

- The community education model should be given further considerations;

- Emphasize on the importance of awareness-raising measures as a continuous cooperation at both national and international levels;

- Relying on more interdisciplinary solutions.

Regarding the general process we draw the attention on the following recommendations:

1. ENISA and EC should address Cyber Security awareness at all levels in different arenas for sharing information.

2. Awareness organisations should pursue Public-Private partnerships in their Educational attempts towards the digital users.

3. NIS in Education community members should target specific stakeholders with different methods and specific content

> Stepping up the national effort on network information security education and training are the main priorities

Our future target will be to search for best practices at country level and pick up top practices to be scaled up at regional, European and international levels.

References

All references were accessed during the period August–November 2013.

Related ENISA papers:

(1) ENISA report (2012), https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/collaborative-solutions-for-network-information-security-in-education

(2) ENISA report (2012) http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/eu-u.s.-event-on-intermediaries-in-cybersecurity-awareness-raising/involving-intermediaries-in-cyber-security-awareness-raising

(3) ENISA report (2011), https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/nis-in-education

Legislation:

(1) EU cyber security strategy ‘An open, safe and secure cyberspace’

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

Articles/websites/multimedia:

(1) http://www.saferinternet.cz

(2) http://www.bsi-fuer-buerger.de
(3) http://www.norsis.no
(4) http://www.sikkert.no
(5) http://www.slettmeg.no
(6) http://www.idtyveri.info
(7) http://www.regjeringen.no/en/dep/jd.html?id=463
(8) Darknet’s motto: http://www.darknet.org.uk/
(9) Internet Security System, Hacking
http://www.iss.net/security_center/advice/Underground/Hacking/default.htm
(10) Search Security by Margaret Rouse (10.2006)
http://searchsecurity.techtarget.com/definition/hacker
(11) https://citizenlab.org/
(12) http://www.hackthissite.org/
(13) https://www.hacking-lab.com/
(14) https://www.owasp.org/index.php/Main_Page
(15) Eric S. Raymond’s Jargon File, The Meaning of ‘Hack’
http://catb.org/jargon/html/meaning-of-hack.html
(16) Exploding the Myth of the ‘Ethical Hacker’ in Forbes by Parmy Olson (31.7.2012)
http://www.forbes.com/sites/parmyolson/2012/07/31/exploding-the-myth-of-the-ethical-hacker/
(17) Schneier on Security, ‘Hiring Hackers’ (10.6.2010)
http://www.schneier.com/blog/archives/2010/06/hiring_hackers.html
(18) Students think hacking is ‘cool’, in Homeland Security News Wire (23. 9.2010)
http://www.homelandsecuritynewswire.com/students-think-hacking-cool
(19) Can hackers be heroes? |PBS Digital Studios (28.3.2013)
https://www.youtube.com/watch?feature=player_embedded&v=NVtrA7juc-w

Annex A: Definitions, quotes and different materials

On hacking

- The word ‘hacking’ has two definitions. The first definition refers to the hobby/profession of working with computers. The second definition refers to breaking into computer systems. While the first definition is older and is still used by many computer enthusiasts (who refer to cyber criminals as ‘crackers’), the second definition is much more commonly used. In particular, the webpages here refer to ‘hackers’ simply because our web-server logs show that everyone who reaches these pages are using the second definition as part of their search criteria.

Internet Security System, Hacking

http://www.iss.net/security_center/advice/Underground/Hacking/default.htm

- Hacker is a term used by some to mean ‘a clever programmer’ and by others, especially those in popular media, to mean ‘someone who tries to break into computer systems’.

(1) Eric Raymond, compiler of *The New Hacker’s Dictionary*, defines a hacker as a clever programmer. A ‘good hack’ is a clever solution to a programming problem and ‘hacking’ is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker, which we paraphrase here as:

- a person who enjoys learning details of a programming language or system;
- a person who enjoys actually doing the programming rather than just theorizing about it;
- a person capable of appreciating someone else’s hacking;
- a person who picks up programming quickly;
- A person who is an expert at a particular programming language or system, as in ‘UNIX hacker’.

Raymond deprecates the use of this term for someone who attempts to crack someone else’s system or otherwise uses programming or expert knowledge to act maliciously. He prefers the term cracker for this meaning.

(2) The term hacker is used in popular media to describe someone who attempts to break into computer systems. Typically, this kind of hacker would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system. For more on this usage, see cracker.

Search Security by Margaret Rouse (10.2006])

http://searchsecurity.techtarget.com/definition/hacker

- Hackctivism? freedom of speech experiments with technology

https://citizenlab.org/

- Hack This Site http://www.hackthissite.org/
- Hacking Lab https://www.hacking-lab.com/
- OWASP hack labs and courses https://www.owasp.org/index.php/Main_Page

Thematic articles

- Eric S. Raymond's Jargon File, The Meaning of 'Hack'

http://catb.org/jargon/html/meaning-of-hack.html

- Exploding the Myth of the 'Ethical Hacker' in Forbes by Parmy Olson (31.7.2012)

http://www.forbes.com/sites/parmyolson/2012/07/31/exploding-the-myth-of-the-ethical-hacker/

- Schneier on Security , Hiring Hackers (10.6.2010)

http://www.schneier.com/blog/archives/2010/06/hiring_hackers.html

- Students think hacking is 'cool' in Homeland Security News Wire (23.9.2010)

http://www.homelandsecuritynewswire.com/students-think-hacking-cool

Multimedia

- Can hackers be heroes? |PBS Digital Studios (28.3.2013)
  https://www.youtube.com/watch?feature=player_embedded&v=NVtrA7juc-w

TP-04-13-119-EN-N

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

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

P.O. Box 1309, 710 01 Heraklion, GREECE
Tel. +30 2814409710
info@enisa.europa.eu
http://www.enisa.europa.eu