enisa
European Network
and Information
Security Agency

BE AWARE, BE SECURE.

SYNTHESIS OF THE RESULTS OF THE FIRST
EUROPEAN CYBER SECURITY MONTH

Acknowledgements

ENISA wishes to acknowledge and thank all Member States and the European Commission Directorate-General for Communications Networks, Content and Technology, which contributed to this document with informal reviews, valuable insights, observations and suggestions. The content would be incomplete and incorrect without their help.

Author of the report: Isabella Santa (ENISA)

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 Awareness raising activities please use the following details:
E-mail: opsec@enisa.europa.eu
Internet: http://www.enisa.europa.eu

For questions related to the European Cyber Security Month, please use the following details:
E-mail: awareness@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.

All images © ENISA, except cover image © David Malan/Getty Images;
and page 5 image © iStockphoto.com/Andreas Kermann

Contents

Index

Abbreviations

ECSM	European Cyber Security Month
ENISA	European Network and Information Security Agency
EU	European Union
DAE	Digital Agenda for Europe
NIS	Network and Information Security
USA	United States of America

List of figures

List of tables

List of graphs

1 Executive summary

For the first time, last October, a European Cyber Security Month took place as a pilot project across Europe. This was as foreseen in the EU–USA Summit final report and in the roadmap produced by the awareness-raising sub-group of the EU–USA Working Group on Cyber-security and Cyber-crime in December 2011. This project was supported by ENISA and the European Commission.

In this first pilot project, the **Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain** and the **United Kingdom** participated in various activities and events throughout October, to raise awareness of cyber security.

Latvia, together with the Council of the European Union, officially supported the project.

The objectives of the European Cyber Security Month (ECSM) were to promote cyber security awareness among citizens, to modify their perception of cyber threats and to provide updated security information through education, good practices and competitions. A diverse range of activities and events targeting different audiences was held throughout Europe. These included: TV and daily radio advertisements; social media campaigns and quizzes with prizes; news articles; conferences; student fairs; roadshows; and round tables.

Each pilot country decided upon the scope and number of activities and events to be organised. ENISA provided guidance and expertise on how to organise information security campaigns, together with tips and advice on how to be safe online. Moreover, the Agency provided promotional material to the participating countries to help promote awareness. This report provides an overview of the activities organised by each country and presents a synthesis of findings on the basis of evaluation and performance information either provided by the pilot countries or gathered by ENISA itself. An overview is provided by aggregating data at European level. Data is also displayed at national level.

The report is structured into four main parts: the overview of the security-related weeks organised at national level across Europe;

- the organisational insights of delivering ECSM initiatives and related achievements;
- the role played by ENISA;
- the lessons learned.

The first part of the report is a global view of the ECSM pilot project. The main findings are:

- the majority of the Member States hold a security week or weeks;
- the proportion of campaigns encompassing general users versus those targeting business users is almost the same;
- a wide variety of key messages are promoted across the different European countries;
- the largest number of events were organised in the fourth week of October;
- all supporting material and communications were produced in the official language of the countries concerned;
- printed materials (38 %) and physical events (25 %) featured in many cases;
- all Member States used a variety of techniques that were fun, exciting and motivating;
- the private sector was involved in six pilot countries;
- the wide variety of delivery channels used suggests the potential value of a multifaceted approach that could match different messages to different media and opportunities across all sectors and countries;
- websites are the most prominent channels of communication used, together with the distribution of giveaways (seven out of eight pilot countries);
- the Member States adopted different methods to assess the effectiveness of ECSM activities — generally, the data gathered can be used to identify very similar key performance indicators.

The second part provides detailed information on the activities and events organised by each country. Quantitative and qualitative information that was captured by the participating countries while measuring the achievements of the ECSM initiatives is reported. A summary table is included for each country to help the reader to view the achievements at national level.

The third part describes the role played by ENISA as coordinator. The Agency was the hub for all pilot countries, not only supporting the ECSM, together with the European Commission, but also providing subject matter expertise and material which helped to get the message out.

The fourth part shows the lessons learned to enable readers to identify key challenges, issues and solutions, making any future ECSM activity more effective. The main findings are as follows.

- Better define the specific audience that is targeted by the awareness initiative in order to tailor the message content to the target group's knowledge or technical aptitude using the most effective communication channels.
- Produce all relevant material in at least all the official languages of participating countries.
- Make press releases available in at least all the official languages of participating countries.
- Produce video clips in different formats in order to allow their use for TV adverts.
- Make sure there are enough staff available during events. Particular attention should be paid to the number of staff available during weekends compared to weekdays.
- Produce giveaways according to the season of distribution (i.e. t-shirts distributed in cold weather did not appear to be a good idea).
- Involve an increased number of private companies to increase impact.
- Deal with changes in plans and keep interested parties informed.
- Ensure media coverage by planning possible interviews in advance. Be prepared for last-minute cancellations.

The analysis carried out in the report lead to the conclusion that the first European Cyber Security Month pilot project was successful, especially because of the engagement, existing good practices and experience of the participating countries.

2 Introduction

Citizens are increasingly relying on the Internet in their everyday lives for banking, shopping, education and a number of other services. It is, therefore, important that they are able to use the Internet in a secure and confident manner.

Making the Internet a better place for all citizens is a shared responsibility, at both European and global level. The EU Cyber Security Strategy, due out in the near future, will set out just how important this is, with concrete proposals to improve digital security. Moreover, the European Union has been working with the USA, and at last year's EU–USA Summit, several steps were agreed to help make the online world secure, on both sides of the Atlantic.

The European Cyber Security Month is an effective instrument for raising awareness about Network and Information Security (NIS).

The main objectives of the European Cyber Security Month are:

- to generate general awareness about Network and Information Security;
- to promote safer use of the Internet for all users;
- to build a strong track record to raise awareness through the ECSM;
- to involve relevant stakeholders;
- to increase national media interest through the European and international dimension of the project;
- to enhance attention and interest with regard to information security through political and media coordination.

This year, eight countries participated in the first European Cyber Security Month: the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain and the United Kingdom. These countries replied positively either to a call for expressions of interest to organise 'Security week' pilot projects sent to all members of the awareness-raising sub-group of the EU–USA Working Group on Cyber-security and Cyber-crime, or to a communication campaign on the project initiated by ENISA.

Over the course of the month of October, a range of local activities and events were held across Europe to raise the security awareness of specific target groups. These included, among others:

- conferences and workshops in Norway, Portugal and Spain;
- media and social media campaigns in Norway and Slovenia;
- non-governmental organization (NGO) round tables in the Czech Republic;
- competitions and quizzes in Luxembourg, Norway and Slovenia;
- roadshows in the United Kingdom.

Each country built on its own existing activities and experience for maximum impact.

2.1 Purpose

The purpose of this document is to consolidate the evaluations of the ECSM activities completed by the pilot countries in addition to providing an analysis of the achievements of the initiatives organised at national level across Europe.

Aiming to provide an integrated perspective across all types of evaluations, the report highlights the results and impact of the ECSM activities, discusses the lessons learned and draws attention to related issues with a view to further enhancing the ECSM's development effectiveness.

In addition, the report concentrates on the learning issues which emerge repeatedly in the countries' evaluations as areas that merit further attention. Among other aims, the report is intended to provide a basis for discussion by the Member States, the European Commission and ENISA on how the ECSM can best be organised in the years to come. All countries are having to face up to a similar challenge, to a greater or lesser extent, namely how to engage citizens and change their information security behaviour.

2.2 Rationale and policy context

This section provides selected information and facts that motivate and explain the decision to organise the first European Cyber Security Month. The main aims of this month include:

- generating general awareness about Network and Information Security;
- promoting safer use of the Internet for all users;
- building a strong track record to raise awareness through the ECSM;
- involving relevant stakeholders;
- increasing national media interest through the European and international dimension of the project;
- enhancing attention and interest with regard to information security through political and media coordination.

Since 2005, the Commission [1] has highlighted the urgent need to coordinate efforts to build the trust and confidence of stakeholders in electronic communications and services. To this end a strategy for a secure information society [2] was adopted in 2006.

On 30 March 2009, the Commission adopted a communication on Critical Information Infrastructure Protection (CIIP) — 'Protecting Europe from large-scale cyber attacks and disruptions: enhancing preparedness, security and resilience' [3], setting out a plan (the 'CIIP action plan') to strengthen the security and resilience of vital information and communication technology (ICT) infrastructures. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities at both national and European levels. This approach was broadly endorsed by the Council in 2009 [4].

In the context of the CIIP action plan, the **European Forum for Member States** discussed and developed European principles and guidelines for the resilience and stability of the Internet ('the principles') [5]. In particular, the principles state that: *Public authorities, with the support of other stakeholders, as appropriate, should strive to educate and raise awareness on the risks associated with Internet-related activities.*

It is recognised that certain categories of stakeholders are not always in a position to properly understand the risks — both for themselves and for the stability and resilience of the Internet as a whole — associated with their Internet-related activities.

Without prejudice to the competences of Member States in the area of culture and education, and taking in the utmost account the principle of subsidiarity, a shared EU approach to such activities, with a view to achieve a global approach, should be sought.

The private sector has an important role to play in supporting public authorities and in providing clear information to all stakeholders, concerning the potential risks of their behaviours for the stability and resilience of the Internet, e.g. unwillingly propagating virus and other malware, having their computers enrolled in a Botnet, etc.

Strengthening education efforts in this area will also have the benefit of producing skilled experts in the needed ICT fields. Education and awareness-raising will also strengthen the preventive abilities of stakeholders, which in turn will help to avoid recourse to ex post or overly invasive security measures. [6]

On these lines, the Digital Agenda for Europe (DAE) [7], adopted in May 2010, and the related Council conclusions [8] highlighted the shared understanding that trust and security are fundamental preconditions for the wide uptake of ICT and therefore for achieving the objectives of the 'smart growth' dimension of the Europe 2020 strategy [9]. The DAE emphasises the need for all stakeholders to join forces in a holistic effort to ensure the security and resilience of ICT infrastructures by focusing on prevention, preparedness and

[1] COM(2005) 229.

[2] COM(2006) 251.

[3] COM(2009) 149.

[4] Council Resolution of 18 December 2009 on a collaborative European approach to network and information security (2009/C 321/01).

[5] European principles and guidelines for Internet resilience and stability (http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf).

[6] European principles and guidelines for Internet resilience and stability (http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf).

[7] COM(2010) 245.

[8] Council conclusions of 31 May 2010 on Digital Agenda for Europe (10130/10).

[9] COM(2010) 2020 and conclusions of the European Council of 25/26 March 2010 (EUCO 7/10).

awareness, as well as to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber attacks and cyber crime. This approach ensures that both the preventive and the reactive dimensions of the challenge are duly taken into account.

These documents provide the rationale and policy context for discussion and cooperation with the Member States and international organisations and, where appropriate, with private sector organisations with the objective of assessing the feasibility of organising a security month in Europe, possibly in coordination with the United States.

Finally, the suggested guidelines foresee the full use of ENISA, as well as other bodies (e.g. the Member States, the Commission and/or industry), to map the principles into concrete and operational activities such as the organisation of the ECSM.

2.3 Scope

The scope of this report is for ENISA to:

- provide an overview of the activities organised by each pilot country;
- present a synthesis of findings on the basis of evaluation and performance information;
- highlight the results and impact of the ECSM activities;
- present the lessons learned;
- draw attention to issues with a view to further enhancing the ECSM's development effectiveness.

2.4 Target audience

This document is intended for organisations, either public or private, which supported the ECSM or intend to do so in the future, as well as IT security managers, professionals and any other target group who attended events and conferences organised across Europe during the month of October 2012.

2.5 Methodology

ENISA gathered information with regard to Member States' ECSM pilot organisations and achievements in two different stages: in the planning phase during Q1–Q2 2012; and in the evaluation phase after 31 October 2012.

ENISA developed templates that focused upon gathering details about security-related weeks organised at national level across Europe. Eight Member States were targeted ([10]) and all of them responded.

The inventory form aimed at extracting pertinent information first on the activities and events planned and then on the results obtained. ENISA participated in three ECSM pilot projects gathering supplementary information.

All information was compiled and then quality checked with the relevant ministries and governmental agencies involved in the organisation of the ECSM pilot. In some cases they were supplemented by additional material, interviews and research carried out centrally by ENISA.

Data has been aggregated by combining data elements from different sources to provide insights and identify patterns in the organisation of security events across Europe and the behaviour of the general public.

([10]) The inventory worksheet template was sent to the ECSM participating countries: the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain and the United Kingdom.

3 The European overview

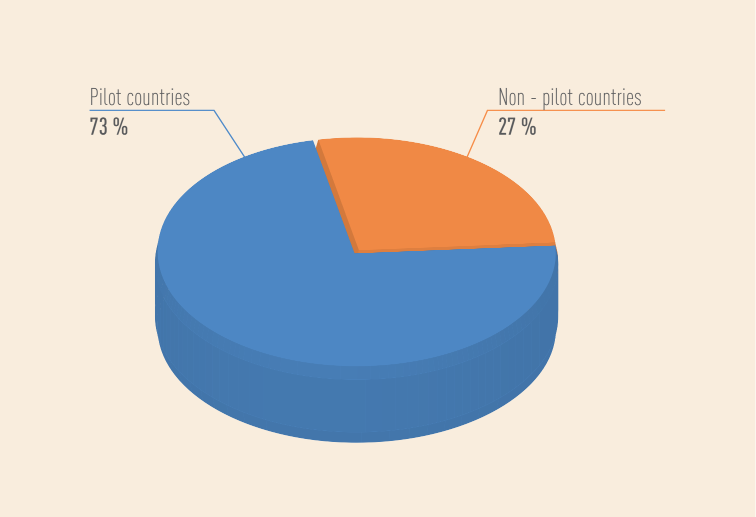
3.1 ECSM pilot projects

All ECSM pilot countries were asked to provide evaluation and performance information regarding any event or activity organised at national level to raise citizens' information security awareness during the month of October 2012.

3.2 Synthesis of findings

This year a total of eight countries participated in the first ever European Cyber Security Month (Figure 1).

FIGURE 1: EUROPEAN OVERVIEW



On 20 January 2012 a call for expressions of interest to organise 'Security week' pilot projects in the context of the ECSM was sent to all members of the awareness-raising sub-group of the EU–USA Working Group on Cyber-security and Cyber-crime, as well as to the representative of the EEA countries. The countries were asked to organise events to raise citizens' information security awareness at national level and eventually to be deployed regionally.

Following this call, six countries responded positively: Luxembourg, Norway, Portugal, Slovenia, Spain and the United Kingdom. The Czech Republic and Romania joined at a later stage following a communication campaign on the project, initiated by the Agency.

These eight countries can be divided between geographical zones as follows: 25 % in northern Europe, 50 % in central Europe and 25 % in southern Europe.

ENISA required either a government/public body of a country or a public–private partnership to organise activities and events to last for at least 1 week.

Each country decided upon the scope and number of activities and events to be organised by building on its own existing activities and experience for maximum impact. The experience in organising such events as well as the 'digital divide' between people in different countries varied from one pilot project to another. The majority of the countries had organised security awareness events in the past. Overall, 37.5 % of the participating countries had run security awareness initiatives before 2008.

Overall, 37.5 % of the participating countries organised activities for the entire month, 25 % for more than 1 week and the others (37.5 %) held events for 1 week.

Over the course of the month of October, a range of local activities and events were held across the eight participating countries: 27 conferences and workshops, two fair stands, seven lectures in schools and five roadshows. The majority of countries (62.5 %) organised social media and online campaigns including competitions.

ENISA provided guidance and expertise on how to organise information security campaigns, together with tips and advice on how to be safe online. Moreover, the Agency provided promotional material to the participating countries to help promote awareness.

The participation of people and the media coverage in all countries was very high.

3.2.1 Participating countries

The following countries participated in the ECSM:

- Czech Republic
- Luxembourg
- Norway
- Portugal
- Romania
- Slovenia
- Spain
- United Kingdom.

One further country and an organisation [11] officially supported the ECSM by reaching and educating citizens, employees and communities through events, activities and/or other campaign distribution methods:

- Latvia
- Council of the European Union.

No data was collected and/or analysed in reference to any of the initiatives organised by the ECSM champions.

[11] Hereafter 'champions'.

3.2.2 2012 events calendar

TABLE 1: 2012 EVENTS CALENDAR

Country	Event type	Target group	Dates	Private sector involved (Y/N)
Czech Republic	Round table	Professionals; NGOs; politicians; public administration; media; industry	22–26 October	N
	Online and media campaign	General public		
Luxembourg	Fair stand	General public	13–21 October	Y
Norway	Conference; seminars; radio advert; online and social media campaign	Citizens; SMEs	All month	Y
Portugal	Conference; workshop	Professionals	1–4 October	Y
Romania	Conference	Professionals; government institutions	All month	Y
	Online and social media campaign	General public		
Slovenia	TV advert; social media campaign	General public	17–31 October	N
	Fair stand	Students		
Spain	Conference	Professionals	All month	Y
	Lecture	Children; parents; teachers; schools; adults; teenagers		
	Social media campaign	General public		
United Kingdom	Roadshow; lecture; online campaign	General public	22–26 October	Y

3.2.3 Goals and objectives of the pilot projects

All over the EU, security events were organised aimed at informing citizens about the importance of information security and highlighting the simple steps people can take to protect their data, whether personal, financial or professional. The main goals and objectives reported were raising awareness, changing behaviour and providing resources to all citizens regarding how to protect themselves online.

3.2.4 Target audience(s)

All countries, with the exception of Portugal, reported events organised for 'all', 'individuals', 'citizens' or 'the general public'. Only a few reported having run a campaign for a very specific target group, such as children, teachers, parents, SMEs etc.

Examples of groups that were targeted by information security events across Europe are listed below [12] (note that the specific names presented here are those provided by the pilot countries, so the groups are not distinctive):

- adults
- children
- citizens
- government institutions
- industry stakeholders
- Internet hotlines
- IT civil servants
- IT professionals (e.g. IT managers, chief information officers, security engineers)
- media
- non-governmental organisations (NGOs)
- parents
- politicians
- public administrations
- schools
- small and medium enterprises (SMEs)
- students
- teachers
- teenagers.

Given the clear overlap between some of the reported groups, it is useful to group similar audiences into three broader categories — general users, young people and business users — as shown in Table 2.

[12] The information is listed in alphabetical order.

TABLE 2: CATEGORISATION OF THE TARGET GROUPS

Main category	Target group
General users	Adults
	Citizens
	Parents
	Schools
	Teachers
Young people	Children
	Students
	Teenagers
Business users	Government institutions
	industry stakeholders
	Internet hotlines
	IT civil servants
	IT professionals
	Media
	NGOs
	Politicians
	Public administrations
	SMEs

The proportion of campaigns encompassing general users versus those targeting business users is almost the same. This is due to the numerous events targeting SMEs and IT professionals. By contrast, the number of security events specifically for young people is about half the number dedicated to general users.

It is worthwhile emphasising the need to better define the specific audience that is targeted by the awareness initiative in order to tailor the message content to the target group's knowledge or technical aptitude using the most effective communication channels. This will maximise the appeal of the message and persuade the audience to take action, especially if the message fits with the target group's interests and needs.

3.2.5 Subject matter

The analysis carried out by ENISA reported that the security topics most often addressed by the national security events across Europe were:

- Internet safety and security
- identity theft
- data protection/privacy
- passwords
- online fraud (scams, phishing)
- cyber crime
- cyber bullying
- social networks
- wireless access
- online child protection
- cyber security
- information security
- cyber threats
- cloud security.

Data available does not allow drawing conclusions with respect to the prioritisation of the above mentioned security topics. However, it appears that some of these topics were more dominant than others, e.g. Internet safety and security, cyber security, online fraud, cyber crime and cyber bullying. It is clear that most of the themes identified had potential relevance to EU citizens in the context of their business and personal lives.

3.2.6 Type of messages used

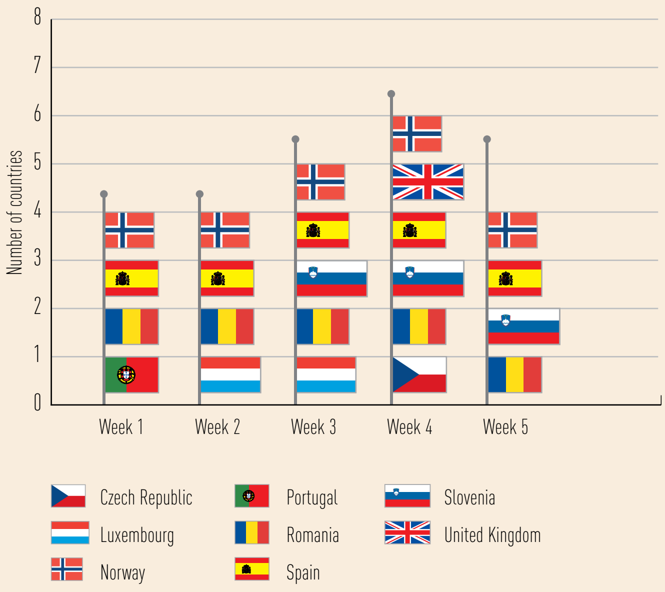
It has not been possible to categorise the messages used in the European countries, mainly because of the variety of styles and languages used.

Data showed that slogans had been created to better promote security events in some countries and increase the level of recognition that citizens had with regard to specific activities. Creating a meaningful and possibly inspiring phrase was shown to be good practice across Europe.

3.2.7 Pilot projects' timeframe

Graph 1 provides an overview of the spread of security pilot projects throughout October, as organised across Europe.

GRAPH 1: WEEKS WHEN ECSM SECURITY EVENTS WERE ORGANISED



Graph 1 shows that the largest number of ECSM activities were organised in the fourth week of October, followed by the third week, and then an equal number of activities were organised in the remaining weeks. This data explains that the pick in media coverage occurred in the third and fourth week of October.

It should be noted that in order to successfully attract the constant attention of the media and the general public, it is important to spread future ECSM activities evenly across the chosen month in order to have awareness activities running continuously for a full month across Europe. This approach would facilitate as well the role played by ENISA as coordinator of the organisation of the ECSM, especially in light of the participation of an increased number of Member States, which appears to be a growing trend.

3.2.8 Languages

To create the greatest impact on citizens, materials were available in the official language(s) of the countries concerned. To this end, ENISA produced guidance material, as well as the ECSM logo, in all 23 official languages to properly engage stakeholders and citizens.

Only two pilot countries used English as well: Portugal and Romania.

3.2.9 Delivery channels

ENISA identified 16 delivery channels that were used to some degree across Europe [13]:

- websites
- giveaways (e.g. key-chains, pens, t-shirts, carrier bags, LED torches and folding flying discs)
- conferences, seminars, workshops, lectures, round tables
- magazines, brochures, booklets and other printed material
- stickers
- flyers, leaflets
- posters
- social networks
- video clips
- newspaper articles, media campaigns
- competitions, draws, tests, quizzes
- exhibitions, expos
- TV, radio
- newsletters
- roadshows
- e-learning.

The wide variety of delivery channels demonstrates that the participating countries choose to deploy multiple channels. It also suggests the potential value of a multifaceted approach that could match different messages to different media and opportunities. Moreover, data from Luxembourg, Slovenia, Spain and the United Kingdom demonstrates that whenever competitions and draws were organised or giveaways were distributed, citizens were more incline to participate in any ECSM activity and instinctively felt more comfortable to receive practical advice on anything from how updating antivirus software to what parental control is.

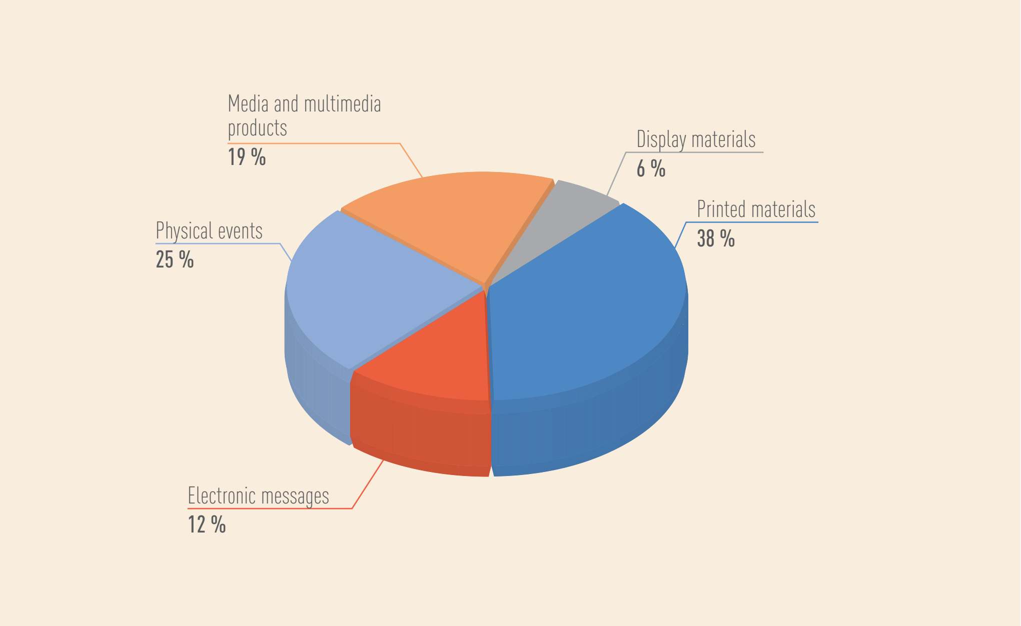
Different colour codes have been used to group the different delivery channels into broader categories, based upon the type of message involved: physical events (yellow), electronic messages (light green), printed materials (light blue), display materials (pink) and media and multimedia products (green).

Figure 2 shows the broad percentages for the delivery categories that were identified. Printed materials (38 %) and physical events (25 %) feature in many cases.

According to the analysis carried out by ENISA, six countries reported using just four delivery methods and two countries used five.

[13] The information is listed in order of popularity.

FIGURE 2: GROUPING OF DELIVERY CHANNELS



The analysis carried out by ENISA reported that, of the delivery channels used to make citizens aware of security issues, websites, giveaways and conferences/seminars/ workshops, etc. were the most common, as illustrated in Graph 2.

In particular, the majority of the pilot countries (seven) used a website as the main channel of communication with their target group. The website is the backbone of ongoing communications and is useful for getting feedback, following which adjustments can be made to the various approaches. Moreover, a website can present content for multiple audiences, is easy to update and maintain, can be easily linked to other information and can be integrated with more than one delivery channel, for example social media, webcasts and e-mail.

Websites, as a communication vehicle, scored the same as the distribution of giveaways. This is a very effective way to attract and interest people.

Finally, the organisation of events comes very close. Usually, conferences, seminars and meetings create high impact and can reach a very wide range of audiences by the careful selection of venues and topics. The experience of Luxembourg, Spain and the United Kingdom, for example, demonstrates how successful and effective physical events could be due to the interactive element of the channel.

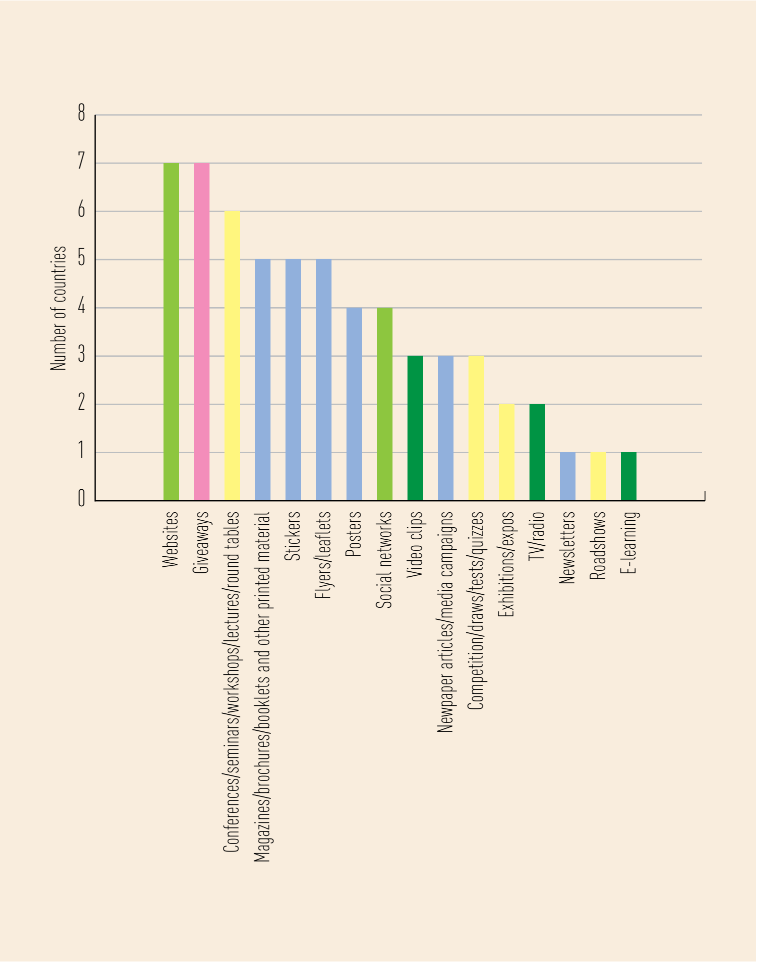
3.2.10 Techniques

In general, all Member States used a variety of techniques which were fun, exciting and motivating in order to catch the attention and stimulate the public they were aimed to. Ways used to make information security events interesting included:

- the use of easy-to-understand terms;
- the use of different messages and activities to ensure awareness was always fresh;
- the use of practical messages;
- the organisation of memorable activities.

For example, Slovenia officially launched its ECSM campaign with a funny video on phishing, Luxembourg organised several activities by delivering the right message to the different visitors of its fair booth at the autumn fair, the United Kingdom used practical messages and tips to engage with the public in high-traffic areas such as shopping centres, railways stations, leisure centres and other public locations.

GRAPH 2: DELIVERY CHANNELS



3.2.11 Costs

ENISA did not gather any information on either the fixed or variable costs connected to the organisation of national awareness initiatives across Europe. This is because data either was not available or not for public distribution.

In any case, it should be considered that costs could vary greatly from one country to another depending on the number of events organised, material produced, availability of resources, previous projects, etc. Considering all these variables and, in particular, the complexity of the campaign organised and its duration, it would be difficult to interpret the calculated average total budget request for an ECSM pilot project.

3.2.12 Measuring the effectiveness of awareness programmes

ENISA asked the pilot countries to provide quantitative and qualitative information captured while measuring the achievements of the ECSM initiatives.

The most common type of data received was quantitative data. These include, amongst others, a focus on metrics such as the number of events organised, number of attendees at events, number of hits on the website or increase in percentage, and number of giveaways distributed. Full details are provided in the sections of the report dedicated to each country.

Different Member States adopted different methods to assess the effectiveness of ECSM activities. Methods used to capture data included, among others, questionnaires, website statistics, general observations, statistics from data centres, data from hotlines, press clippings, press releases and number of people trained.

Generally, the data which have been gathered could lead to very similar key performance indicators. This indicates that what the pilot countries found effective is broadly similar.

Table 3 illustrates different performance indicators that were mostly used across Europe.

TABLE 3: PERFORMANCE INDICATORS USED ACROSS EUROPE

No	Performance indicator	Approach
1	Number of materials distributed per week/month	Process improvement
2	Number of materials distributed per edition	Process improvement
3	Number of events listed per month	Process improvement
4	Number of people attending events per location	Process improvement
5	Number of hits on website per month	Process improvement
6	Number of downloads per video clip	Process improvement
7	Mean time between discovery and notification of an attack and/or new threat	Attack resistance
8	Number of security incidents per month	Efficiency and effectiveness
9	Etc.	Etc.

Each performance indicator can be redirected to a different approach [14].

- Process improvement: this approach assesses the effectiveness of the campaign by looking at its activities. These measures are easy to define and gather: however, they do not directly measure whether the end result has improved security.
- Attack resistance: this approach measures how resistant users are to a potential attack. This approach provides evidence on the level of awareness of the people concerned. However, the number of attack scenarios is quite high, and the measure will be specific to the scenario it is testing.
- Efficiency and effectiveness: this approach focuses on the actual experience of security incidents. The data can be gathered through the overall security incident but does not necessarily give a true reflection of security awareness. It is not just awareness that determines whether incidents occurred. However, in the long term, the trend can be a good indicator of awareness.
- Internal protection: this approach assesses how well users are protected against threats. The advantage of these measures is that they provide direct evidence of users' behaviour. Often, though, the campaigns are aiming to change behaviour. This can result in many metrics.

The data should be continually captured across all pilot countries (as performance measurement and monitoring the effectiveness of an initiative should be done during and after execution), and should ideally be reviewed with a view to how future activities might be improved and made more effective. This information should be combined with the results derived from the evaluation metrics. The ECSM pilot projects' objectives need to be revisited by each country in light of the effectiveness results. Reviewing the objectives allows for a serious assessment to take place.

To this end, a recent study conducted by ENISA [15] reported that the evaluation of an awareness campaign or programme is essential to understand its effectiveness, as well as to use the data as a guide to adjust the initiative to make it even more successful. This report suggests how to define indicators to measure the success of an awareness programme as well as how to conduct evaluations. Below there are some of the indicators which were identified and could be used to measure future ECSMs.

[14] *Information security awareness initiatives: Current practice and the measurement of success*, ENISA, July 2007.

[15] *The new users' guide: How to raise information security awareness*, ENISA, November 2010, available at http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide

TABLE 4: EXAMPLES OF PERFORMANCE INDICATORS

No	KPIs (*)
1	% of budget spent on awareness training
2	% of time spent on awareness training per FTE
3	Age of employees attending an awareness training/average age of total employees
4	Cycle time in days between organisation of awareness activities and completion of campaign
5	Number of FTEs IT-security trained/total users
6	Number of qualified hits/month
7	Total cost of awareness initiative per year
8	Total costs of awareness training per FTE
9	Total personnel cost of the planning and management awareness initiatives
10	% customer satisfaction with service delivery (i.e. timelines and quality)
11	% employee capability to perform roles
12	% employee satisfaction
13	% increase confidence for elderly
14	% senior management/executives; middle management/professionals; operational works/staff that attended management development programmes
15	% senior management/executives; middle management/professionals; operational works/staff that received a security review
16	% service delivery performance targets achieved
17	% stakeholder satisfaction with communication about the programme
18	% stakeholder satisfaction with governance arrangements
19	% stakeholder understanding of initiative benefits
20	% stakeholders' resistance to change
21	% stakeholders' satisfaction with ability of the system to meet business requirements
22	% employees understanding their role in achieving security goals
23	Average number of learning days per employee
24	Average personnel cost per FTE for the process 'change management'
25	Average personnel cost per FTE for the process 'raising awareness'
26	Frequency/relevance of surveys
27	Number of benefits realised as stated in business case
28	Number of employees per 'develop and counsel-learning' FTE
29	Number of changes in managers' roles
30	Number of changes in staff activities
31	Number of correct answers on self security assessments/total questions
32	Number of employees in charge of development/total employees
33	Number of FTEs for the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations
34	Number of participants in the awareness survey/total employees
35	Number of self security assessment done/year
36	Total cost of the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations

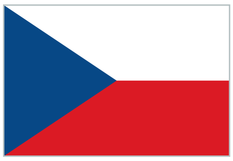
No	KPIs (*)
37	Total internal personnel cost of the process 'develop and counsel-learning' per EUR 1 000 cost of Continuing operations
38	Contribution of ICT training to value added per person engaged in % points
39	Number of employees who passed the exam or certification/total Number of employees
40	Number of organisations adopting the tools/year
41	Number of people who passed the exam or certification/total Number of people interviewed
42	Number of tools downloaded/month
43	Number of topics on security in high school and education/total topics
44	Number of topics on security in standard primary and secondary school education/total topics
45	% of budget allocated to awareness training
46	% of employees born after 1950
47	% of businesses with 10 or more employees using Internet
48	Number of access lines and channels in total/per 100 inhabitants
49	Number of households with access to home computer/country
50	Number of households with access to Internet/country
51	Number of mobile subscribers in total/per 100 inhabitants
52	Number of broadband subscribers/per 100 inhabitants
53	Training cost per FTE
54	Cycle time in days to resolve a security problem
55	Mean time between discovery and notification of a new threat
56	Number of identified fault/year
57	Number of alerts, advisories, notifications, recommendations/month
58	Number of communications with other countries/year
59	Number of systems without implemented password policy/total Number of systems
60	Number of tokens/certificates/eID cards issued/total population
61	Number of reported incidents per category/year
62	Number of certification scheme adopted by local or international companies
63	Number of e-government projects using the standards/total projects
64	Number of editions/year
65	Number of events listed/month
66	Number of material distributed/edition
67	Number of material distributed/year
68	Number of people attending awareness trainings per campaign
69	Number of training days per staff/year
70	Number of unique visitors/month
71	Time to organise an awareness initiative

(*) Most KPIs are expressed on a pro rata basis (i.e. number of units per FTE or per EUR 1 000 of spend) rather than in absolute terms.

% = percentage; FTE = full-time equivalent.

4 Pilot countries

4.1 Czech Republic



The Czech Republic participated in the ECSM from 22 to 26 October 2012.

The Ministry of the Interior of the Czech Republic supported and promoted the European Cyber Security Month in the Czech Republic.

Activities and events were scheduled to take place as follows.

- A round table of NGOs engaged in the field of online child protection, Czech Internet hotlines, computer security incident response teams (CSIRTs) and industry stakeholders. The event was organised under the auspices of Mr Kubice, Minister for the Interior of the Czech Republic, and Mrs Simunkova, the government's Commissioner for Human Rights.
- Online outreach and promotion plans through the website http://www.saferinternet.cz and newsletters.
- Media campaign.

The Czech Safer Internet Centre (NCBI) joined the ECSM pilot projects initiated by ENISA to stay safe and secure online. The NCBI organised the first round table of NGOs, public administration representatives and organisations operating CSIRTs/CERTs (computer emergency response teams) in the Czech Republic.

The event took place on 26 October 2012 in Prague under the auspices of Mr Kubice, Minister for the Interior of the Czech Republic, and Mrs Simunkova, the government's Commissioner for Human Rights. The Director of CERT-EU, Mr Freddy Dezeure, addressed the attendees of the round table with his speech.

The main objective of the round table was to increase mutual information exchange and cooperation between organisations and companies that are active regarding education in and promotion of online literacy, safer use of the Internet, online crime prevention and dealing with socially pathological phenomena on the Internet, or that operate as hotlines dealing with Internet threats.

At the meeting, attention was paid to the following issues:

- the specific activities of individual organisations and the possibilities of closer cooperation, and the coordination problems of children, their parents and teachers in the area of online communication;
- possibilities and ways of strengthening cooperation among NGOs, relevant public institutions and bodies active in criminal proceedings regarding protection of children's rights on the Internet and preventing online crime;
- options and ways for a common approach to dealing with politicians and public administrations in increasing protection for Internet users, especially children.

Visitors to the http://www.saferinternet.cz website were informed about the ECSM initiatives organised in the Czech Republic. This website was the main online source of information, and traffic increased significantly to 2 824 visitors, 70.25 % of whom were new visitors. The same information about the ECSM activities was also distributed to the 6 500 Czech schools via the Safer Internet newsletter.

TABLE 5: CZECH REPUBLIC SUMMARY TABLE

Czech Republic	
Government/national entities taking part in the ECSM	Ministry of the Interior of the Czech Republic
Private sector involved	No
Duration	22–26 Oct. 2012
Languages used	CZ
Number of events organised	1 (round table)
Number of attendees	> 30
Number of locations	1 (Prague)
Target audience	NGOs; Czech Internet hotlines; CSIRTs; Industry stakeholders; Politicians; Public administration; Media
Number of other activities organised	2 (online and media campaigns)
Subject matter	Internet safety; Online child protection; Cyber bullying
Delivery channels	Conference; Giveaways; Stickers; Newsletter; Website; Media
Number of ENISA giveaways distributed	464

4.2 Luxembourg

Luxembourg participated in the 'Security week' pilot project with its annual campaign focused this year (2012–13) on risks related to bullying and stalking.

The 'BEE SECURE' initiative from the Luxembourg government was present with its 80 m^2 fair booth at the autumn fair from 13 to 21 October 2012. Security tips were illustrated to the visitors either by talking through some of the available brochures and leaflets or by helping the visitors test how strong their password was through a computer available at the stand. Tablets were at the disposal of citizens interested in taking part in competitions and draws. A table was organised to entertain kids while their parents were visiting the stand. The fair attracted more than 43 000 visitors. The stand was visited by thousands of citizens, emptying the booth of campaign material. During the opening ceremony the Grand Duke of Luxembourg paid a visit to the stand.

TABLE 6: LUXEMBOURG SUMMARY TABLE

Luxembourg	
Government/national entities taking part in the ECSM	BEE SECURE, an initiative of the Ministry of Education, Ministry of Family and Integration and Ministry of the Economy and Foreign Trade, operated by SNJ (the National Youth Agency) and SMILE (Security Made In Lëtzebuerg)
Private sector involved	Yes
Duration	13–21 Oct. 2012
Languages used	FR, DE
Number of events organised	1 (fair booth)
Number of attendees	43 000 at the fair, ~ 10 000 at the stand
Number of locations	1 (Luxembourg)
Target audience	Citizens
Number of other activities organised	2 (distribution of posters and flyers through partners)
Subject matter	Internet safety and security; Strong passwords; Online child protection; Cyber bullying; Stalking
Delivery channels	Fair stand; Giveaways; Stickers; Leaflets; Website; Competitions, draws; Brochures and other printed material; Posters
Number of posters distributed	3 300
Number of ENISA giveaways distributed	9 250
Number of other giveaways distributed	18 556
Number of flyers and activity reports distributed	6 350
Number of partners' flyers distributed	Hundreds

4.3 Norway

Norway participated in the European Cyber Security Month by organising activities and events for citizens and SMEs throughout the month of October.

The Norwegian Centre for Information Security (NorSIS) ran the 'Stopp. Tenk. Klikk.' (Stop. Think. Connect.) campaign during October to celebrate the European Security Month. The events and activities were part of a national public awareness campaign aimed at increasing the understanding of cyber threats and enabling Norwegian citizens to be safer and more secure online.

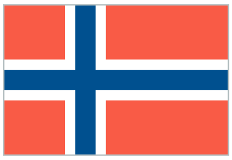
The campaign's main objective was to help all citizens become more aware of threats and, in particular, better understand how to protect:

- personal information and identity by using strong passwords;
- businesses by keeping security software current.

The government and private organisations welcomed the initiative.

Activities and events were scheduled to take place during the entire month of October as follows.

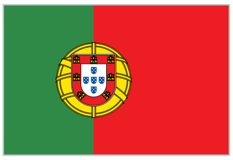
- Kick-off event by means of a conference. The opening address was given by the Minister for Government Administration, Reform and Church Affairs, Mrs Rigmor Aasrud. Video clips were used during the day.
- Daily radio advertisements.
- Internet advertisements.
- Articles in the news.
- Distribution of educational packages to SMEs, including presentations, videos, posters and gadgets raising the information security awareness of approximately 60 000 Norwegian employees.
- Website campaign (http://www.sikkert.no). 18 500 visitors were registered for the entire period.
- Social media campaigns on Facebook (Nasjonal Sikkerhetsmåned) and Twitter (#sikkerhetsmåned).
- More than 37 conferences and seminars were held throughout Norway, from Narvik in the north to Oslo, Trondheim, Gjøvik, Stavanger and several other locations in the country.
- Internal seminars/meetings, with volunteer speakers, organised at Norwegian companies through the 'National Security Month' project and administered through http://www.sikkert.no. Companies chose the topic to be covered during the seminar/meeting from 30 different presentations.
- NorSIS gave 30 presentations at different seminars and conferences.



An education package was distributed to 115 businesses in Norway during the month of September in order to have training activities organised in-house during the month of October. The package included the following: presentations, e-learning, brochures with security tips for employees, posters, videos, gadgets.

TABLE 7: NORWAY SUMMARY TABLE

Norway	
Government/national entities taking part in the ECSM	Norwegian Centre for Information Security
Private sector involved	Yes
Duration	Whole of October 2012
Languages used	NO
Number of events organised	37 (conferences and seminars)
Number of attendees	Approximately 2 000–2 500
Number of locations	12 (Bergen, Bærum, Bodø, Gjøvik, Kristiansand, Lillehammer, Narvik, Nittedal, Oslo, Skien, Stavanger, Trondheim)
Target audience	Citizens; SMEs
Number of other activities organised	7 (distribution of posters and educational material for SMEs; radio and Internet advertisements; video clips; articles on magazines and newspapers)
Subject matter	Internet safety; Updating programs; Privacy; Passwords; Encryption; Security software
Delivery channels	Conferences; Seminars; Giveaways; Stickers; Educational packages for SMEs including e-learning, presentations, videos, security tips, posters and gadgets; Leaflets; Posters; Website; Internet advertisement; Video clips; Social media; Articles; Press releases; Radio advertisements
Number of posters distributed	1 000
Number of ENISA giveaways distributed	1 098
Number of radio advertisements' listeners	Approximately 5 000 000



4.4 Portugal

The National Security Office, in collaboration with ShadowSEC and the United Nations Interregional Crime and Justice Research Institute (UNICRI), organised the second edition of InfosecDay under the auspices of the European Cyber Security Month.

Portugal participated in the 'Security week' pilot project by organising a conference and a series of workshops aimed at discussing the main national and international trends and emerging risks regarding cyber security. The events were held on 1–4 October 2012 in Lisbon. A series of workshops were held on 1–3 October and a conference on 4 October. The events were open to IT professionals, civil servants and government institutions.

TABLE 8: PORTUGAL SUMMARY TABLE

Portugal	
Government/national entities taking part in the ECSM	National Security Office (GNS)
Private sector involved	Yes
Duration	1–4 October 2012
Languages used	PT, EN
Number of events organised	4 (workshops and conference)
Number of attendees	240
Number of locations	1 (Lisbon)
Target audience	IT professionals; IT civil servants; Government institutions
Number of other activities organised	NA
Subject matter	Cyber crime legislation; National cyber security strategy; Cyber threats; Digital investigation; Data protection; ISO 27001; Cloud security; Responding to security incidents; Public-private partnerships; Software development
Delivery channels	Conferences; Seminars; Giveaways; Leaflets; Website; Brochures and other printed material; Stickers
Number of posters distributed	NA
Number of ENISA giveaways distributed	708

Over 4 days, the Portuguese events saw 240 participants (83 attending the workshops and 157 the main conference) from approximately 75 companies and 16 speakers.

The main theme and agenda of the events were very well received by all attendees, as well as the quality of the information shared and the time for discussions which was allowed.

The second edition of InfosecDay received excellent press coverage. The website dedicated to the events had over the period a total of 341 visits with an increase of new visits by 67,16 %.

4.5 Romania

Romania participated in the European Cyber Security Month (ECSM) by organising various activities to raise Romanians' information security awareness throughout the month of October, changing the original plans to cover only the period 15–19 October 2012. This was mainly due to the fact the organiser recognised that social media and online campaigns would have been more effective and successful if run for at least a period of four weeks.

The Romanian CERT organised various activities to raise information security awareness as follows.

- Cyber Threats 2012: public conference on cyber security.
- Social networks and online campaigns: information security advice and articles were provided to visitors to the website http://www.cert-ro.eu and the relevant Facebook, Twitter, Google+ and LinkedIn accounts.
- Press releases to inform the population about events organised by CERT-RO during the month.

4.5.1 Cyber Threats Conference 2012

The conference was dedicated to raising awareness among Internet users about the dangers of cyber attacks, especially in the financial and banking sectors. This year, 202 people attended the conference, which through panel discussions covered the following:

- the implications of operational and security risks generated by IT activities and communications in the banking sector;
- cyber threats and the existing solutions for data protection.

4.5.2 Online and social media campaigns

Various online and social media campaigns ran during the month of October.

A dedicated section of the CERT-RO website (http://www.cert-ro.eu/ECSM2012.php) was developed and populated with information about the ECSM, its material and posts (18 in total) on matters related to Internet security. The posts consisted of articles, guides, tips and advice, and press releases. Moreover, 15 media articles in Romanian were published and also distributed via social media channels such as Facebook, Twitter, Google+ and LinkedIn.

Social media were used to share information on the ECSM and the activities scheduled in Romania, as well as to illustrate, in an engaging way, matters regarding information security and the related risks and threats. Tweets were posted in Romanian and English.

TABLE 9: ROMANIA SUMMARY TABLE

Romania	
Government/national entities taking part in the ECSM	CERT-RO
Private sector involved	Yes
Duration	Whole of October 2012
Languages used	RO, EN
Number of events organised	1 (conference)
Number of attendees	202
Number of locations	1 (Bucharest)
Target audience	IT professionals; IT civil servants; Government institutions
Number of other activities organised	2 (online and social media campaigns)
Subject matter	Cyber security
Delivery channels	Conference; Social networks; Website; Media; Video clip; Posters
Number of posters distributed	200
Number of ENISA giveaways distributed	NA
Number of other giveaways distributed	222

4.6 Slovenia

Slovenia participated in the ECSM by organising various activities to raise Slovenians' information security awareness for 2 weeks (17–31 October 2012).

The Slovenian CERT organised various activities to raise information security awareness as follows.

- Facebook campaign: via this social media platform, information security tips were provided to visitors to the page. Quizzes about information security took place and prizes were distributed. By 30 October, 250 people had participated in the quiz, registering 2 200 new 'likes' on the dedicated Facebook page.
- Television campaign: TV adverts were broadcast for the entire period of the campaign. The adverts, reminding people how to protect from online fraud, encouraged viewers to visit the educational portal 'Safe on the Internet' and get more info about information security.

- Students' fair (23–25 October 2012): the Slovenian CERT was present with its booth at the students' fair. Leaflets and The ABC of online safety booklet were distributed. Visitors to the stand had the chance to participate in a quiz game: 'Are you a web detective?' A clip on Nigerian scams was launched during this initiative [16].
- Three new video clips were launched in collaboration with two famous Slovenian comedians. By 30 October, the videos as a whole had received more than 18 600 views on YouTube [17].

On 17 October, Slovenia officially launched its ECSM campaign with a funny video on phishing [18], a Facebook quiz, TV ads and banners. In the first 24 hours, the website http://www.varninainternetu.si/ had more than 2 700 views, with a total increase in traffic of 200 %. During the entire campaign the website got more than 18 000 unique visitors.

TABLE 10: SLOVENIA SUMMARY TABLE

Slovenia	
Government/national entities taking part in the ECSM	ARNES SI-CERT
Private sector involved	No
Duration	17–31 October 2012
Languages used	SL
Number of events organised	1 (fair booth)
Number of attendees	More than 21 000 students and young adults visited the students' fair. The booth was visited by around 200 people who also participated in the quiz
Number of locations	1 (Ljubljana)
Target audience	Citizens; Students
Number of other activities organised	3 (social media campaign; TV adverts; online quizzes)
Subject matter	Online safety; Online fraud (Nigerian scams, phishing, fake online stores)
Delivery channels	Social media (Facebook, Twitter and YouTube); Online campaigns (i.e. web banners, articles on national online news portals); TV adverts; Fair stand; Video clips; Giveaways; Quizzes, competitions; Leaflets; Booklets
Number of posters distributed	NA
Number of ENISA giveaways distributed	500

[16] http://www.youtube.com/watch?v=blDPpm6QGXM&list=UU4-56IdnZZN3sizLeqbMgVw&index=1&feature=plcp

[17] The video about fraudulent online stores is available at http://youtu.be/iPHHOEsTvKQ

[18] http://www.youtube.com/watch?v=A0SQp9rEots

4.7 Spain

Spain participated in the European Cyber Security Month (ECSM) by organising a conference for information security professionals and several activities for children, teenagers and adults throughout the month of October 2012.

Inteco [19] participated in the ECSM by organising the sixth ENISE (International Meeting on Information Security). The conference took place on 23–24 October 2012, registering 386 attendees and 18 000 more by video streaming.

Moreover, activities and events to raise the information security awareness of children, teenagers and adults were scheduled to take place throughout the month of October as follows.

- 'What do you know about security?' story and drawing competitions for children from 5 to 12 years old. In the **drawing category**, 15 schools participated with 525 drawings. In the **story category**, 22 schools participated with 350 stories.
- 'Choose your mascot' campaign: this initiative tried to teach basic security concepts to students from 5 to 8 years old. The children chose a mascot from the Menores OSI website who explained information security to them. A total of three schools participated in this pilot project. Before deploying this initiative to all schools, pros and cons will be analysed and material reviewed.
- Lectures about Internet security and social networks focused on children, teenagers, parents and teachers. These lectures took place in several schools all over Spain: six lectures in three schools, with 326 attendees (309 children and 17 parents and teachers). The schedule was as follows:
  - » 9/10/2012 — two lectures to students at San Juan de la Cruz School (León);
  - » 9/10/2012 — one lecture to parents and teachers at San Juan de la Cruz School (León);
  - » 15/10/2012 — two lectures to students at Virgen Blanca School (León);
  - » 31/10/2012 — one lecture to students at Don Bosco School (León).
- Social media campaigns: information security tips were advertised throughout Facebook and **Tuenti** [20]. Various adverts were created: three on Tuenti registering an increase of 20 followers; 12 on the **Facebook page 'OSI'** registering an increase of 1 830 followers; and 12 on the **Facebook page 'Pienso, luego clico'** registering an increase of 1 443 followers.

Menores OSI
¿CUÉNTAME QUÉ SABES SOBRE SEGURIDAD EN INTERNET?
MODALIDAD DIBUJO

These activities were organised by Inteco through OSI (http://www.osi.es), its national security helpdesk for citizens. This website received 102 954 visitors, an increase of 21 %.

TABLE 11: SPAIN SUMMARY TABLE

Spain	
Government/national entities taking part in the ECSM	Instituto Nacional de Tecnologías de la Comunicación (Inteco)
Private sector involved	Yes
Duration	Whole of October 2012
Languages used	ES
Number of events organised	7 (lectures and conference)
Number of attendees	722, and 18 000 virtual attendees
Number of locations	1 (León)
Target audience	Information security professionals; Children; Teenagers; Adults; Parents; Teachers; Schools
Number of other activities organised (competition, social media campaign, etc.)	3 (competition, social media campaign and 'choose your mascot" campaign)
Subject matter	Information security
Delivery channels	Conference; Lectures; Social networks; Competitions; Giveaways
Number of posters distributed	NA
Number of ENISA giveaways distributed	1 004

[19] http://www.inteco.es

[20] Tuenti is a Spain-based, invitation-only private social networking website for students and young people.

4.8 United Kingdom

The United Kingdom participated in the 'Security week' pilot project by organising initiatives and events in five major cities across the country from 22 to 26 October 2012.

Get Safe Online — the UK's leading source of free, practical, expert information and advice on online safety — organised the seventh annual Get Safe Online Week under the auspices of the ECSM. This year's theme was **'Click & Tell'**, designed to get as many people as possible across the UK to pass on online safety tips to friends, family, colleagues, neighbours, vulnerable people, or anyone who could benefit from the advice.

The focus of Get Safe Online Week was a roadshow visiting five major UK cities (Cardiff, London, Leeds, Edinburgh and Belfast), engaging with the public in high-traffic areas such as concourses, shopping centres, railway stations, leisure centres and other public locations. The message was also cascaded by Get Safe Online's partner community as well as other interested parties. A number of celebrities and other well-known personalities were recruited to endorse this important message.

The campaign reached 124 160 943 citizens. The Get Safe Online team visited the following locations.

Cardiff

- Cardiff central station: from early in the morning until 9.15 a.m. the team gave out leaflets and giveaways to commuters, with a fantastic response. The information staff at the station wore Click & Tell badges all day.
- Queens Arcade: a stand was set up in the shopping centre, where leaflets were handed out to the good shoppers of South Wales along with Click & Tell foam hands and memory sticks. The coach was parked outside the arcade all day, and free, practical advice was given on anything from how not updating antivirus software could be making a lady's computer slow down, to what parental control software is available for iPads, etc. Mr David Jones, Secretary of State for Wales, visited the coach to chat with the team and a group of children from St Cadoc's R. C. Primary School in Llanrumney, Cardiff. The children also chatted with the Get safe Online team and its guest experts about online safety live on BBC Radio Wales.

London

- Waterloo station: a team of seven pitched the Click & Tell pop-up display at Waterloo station, remaining in situ until 10 a.m. offering advice to commuters and handing out leaflets and goodies.
- Admiralty Arch, Trafalgar Square: the coach parked at Admiralty Arch, Trafalgar Square where a steady flow of people dropped into speak to the experts on board.
- Sir John Cass Foundation Sixth Form College in Stepney Green: a couple of people from the content team addressed the school assembly about online safety. Later in the day, the Get Safe Online team entertained four of the college's youngsters on the coach in the afternoon — also catching up with Parliamentary Secretary to the Cabinet Office Chloe Smith, who was visiting at the same time. The minister also met supporters from SOCA, Symantec, the Metropolitan Police, HMRC, PhonePayPlus, Gumtree, Three and our government ambassadors from the Cabinet Office and the Department for Business, Innovation and Skills.

Leeds, West Yorkshire

- Leeds station: the team offered advice to the commuters of West Yorkshire, who were very receptive of the initiative and the online safety messages. Thousands of flyers and giveaways were distributed.
- Briggate: the Click & Tell coach was parked in one of the city's main shopping streets, where the team engaged with the public on all aspects of online safety.

Edinburgh

- Edinburgh station: the team talked to the commuters about the importance of Internet security.
- St James Shopping Centre: leaflets, t-shirts, foam hands and good advice were distributed in the true spirit of Click & Tell. Again, some themes seemed to predominate, with questions about safe emailing and keeping children protected.
- Castle Street: the coach parked across Castle Street, where citizens were reminded how to stay safe and secure online.

Belfast

- Europa bus centre and Great Victoria Street station: from 8 a.m. to 9.30 a.m.
- City Hall: from 12 noon to 2 p.m.
- Tesco Extra Knocknagoney Road: from 2.30 p.m to 3.30 p.m.
- In all three locations, leaflets and giveaways were distributed and well received, probably because some 60 % of the population has been directly affected by online crime, one of the worst records in the United Kingdom.
- Queen's University library: the team chatted with students about a number of aspects of online safety.

During the Get Safe Online Week, the website http://www.getsafeonline.org/ had more than 25 000 unique page views, with a total increase of 57 % compared with the previous week [21].

The amount of traffic gained from referring websites increased by over 75 % in a week – indicating that other websites were helping to promote the Get Safe Online website and the events organised in the context of the Get Safe Online Week.

Almost 85 % of the people who visited the website during that week had not visited it previously, indicating excellent reach for the programme.

TABLE 12: UNITED KINGDOM SUMMARY TABLE

United Kingdom	
Government/national entities taking part in the ECSM	Get Safe Online
Private sector involved	Yes
Duration	22–26 October 2012
Languages used	EN
Number of events organised	2 (roadshow and lecture)
Number of attendees	Not provided
Number of locations	5 (Cardiff, London, Leeds, Edinburgh, Belfast)
Target audience	Citizens; Students; Schools
Number of other activities organised	6 (distribution of leaflets, posters, giveaways, printed material and brochures; online campaign)
Subject matter	Get safe online
Delivery channels	Roadshow; Lecture; Leaflets; Posters; Giveaways; Printed material, brochures; Website, blog
Number of posters distributed	5 000
Number of ENISA giveaways distributed	NA
Number of other giveaways distributed	10 000 Trend Titanium licenses; 1 000 t-shirts; 1 000 folduo flying discs; 2 000 Symantec USB sticks
Number of flyers distributed	10 000

[21] The website http://www.getsafeonline.org/ had 61 248 page views up from 36 595 (+ 67.37 %) the previous week.

5 Role played by ENISA

ENISA supported the organisation of the European Cyber Security Month pilot projects in various ways, as:

- coordinator of the organisation of the ECSM;
- hub for all participating countries;
- collector of available material and generator of synergies between pilot countries;
- subject-matter expert on how to organise information security campaigns;
- facilitator of common messaging within the participating countries by providing tips and advice on how to be safe and secure online;
- creator of the ECSM brand and related marketing plan;
- distributor of promotional material (about 15 000 giveaways and 10 000 posters).

The Agency coordinated the organisation of the 2012 ECSM, trying to become the hub for all pilot countries by providing suggestions, replying to enquiries and generating synergies between countries when possible. For example, the interaction between Luxembourg and Norway and that between the United Kingdom and Slovenia, along with Norway, demonstrated how successful synergies could be.

ENISA provided guidance and expertise on how to organise information security campaigns by using its methodology on how to prepare and implement awareness campaigns [22], and developed a series of common messages and material to help Member States prepare their cyber security education and awareness campaigns in a similar ways in the context of the European Cyber Security Month. This material was recognised by all countries as an important tool in reaching people and getting them to change their behaviour, or to reinforce good behaviour.

This material included:

- tips and advice to provide in-depth information on how to stay safe in a variety of online settings, for example on social networking sites, on gaming sites and on your mobile device;
- ECSM posters;
- ECSM web banners;
- ECSM certificate of appreciation template (white background and coloured background);
- ECSM letterhead;
- ECSM PowerPoint template;
- ECSM name tags form;
- ECSM video clip [23].

Moreover, the Agency produced promotion material for the Member States to help promote awareness messages and also helped to identify speakers for events.

[22] *The new users' guide: How to raise information security awareness*, ENISA, November 2010, available at http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide

[23] As of 15 November 2012, the ECSM clip had 1 099 views. The video is available at http://www.youtube.com/watch?v=q00uIu0YWoo A short version of the same clip had 870 views. The video is available at http://www.youtube.com/watch?v=7d9l6ua3p0s

5.1 Brand marketing plan

A series of activities were planned to market the European Cyber Security Month project.

5.1.1 Visual identity

To strengthen visibility and public recognition of the European Cyber Security Month, ENISA created a visual identity including a logo, a colour chart, typography rules, guidelines on use of imagery, design templates and a manual of formal guidelines on the proper use of these elements.

The design was created following consultation with the Member States and the European Commission.

5.1.2 Slogan

The slogan 'Be aware. Be secure.' was created to give the project an identity and a positive image. It was used in some of the material and giveaways produced for the European Cyber Security Month project. The slogan always appeared when information security tips were displayed in posters and in any other relevant material.

5.1.3 Advertising campaign

The European Cyber Security Month featured a diverse range of activities and events, and as part of the build-up ENISA launched a campaign that gave people the chance to feature in advertisements and other promotional material by sending in photographs of themselves.

ENISA aimed to bring the slogan of the project, 'Be aware. Be secure.', to life.

5.1.4 Social media

Dedicated social media accounts were created as a source of useful advice about information security in general, as well as tips and recommendations on how to protect your PC and personal and business information. The accounts provided information on the activities and events organised in each of the pilot countries.

Accounts were set up and activated on the following social networking sites:
- Twitter
- Facebook
- LinkedIn.

Moreover, the ENISA social media channels [24] were used to advertise the ECSM activities. More than 2 300 unique page views [25] were originated from ENISA social media traffic in relation to the European Cyber Security Month. This data represents almost 25 % of the total unique page views of all ENISA social media traffic for the period 18 September 2012 – 31 October 2012.

EUROPEAN
CYBER
SECURITY
MONTH

[24] ENISA launched its social media channels on 19 September 2012. Social Media channels officially launched on 19 September included Twitter and Facebook. LinkedIn was an automatically generated page already active and YouTube page was created on 6 July 2012.

[25] Data related to period 18 September 2012 – 31 October 2012.

5.1.4.1 Facebook campaigns

ENISA ran six Facebook campaigns in order to make citizens aware of the project and its activities and build brand recognition. Campaigns were organised at European and Member States' level targeting: Luxembourg; Norway; Portugal; Slovenia; and Spain.

All campaigns targeted the same audience and were created in the language of the relevant country. The duration of each campaign was set according to the length of the activities planned in the targeted pilot countries. All campaigns pointed to the dedicated ENISA webpages.

The Facebook campaigns, along with the press releases and the new items published by the Agency during the months of September and October, registered a total of 44 363 unique page views [26], an increase of 5.44 % compared to the previous 2 months.

Moreover, the media campaign and the video of Vice President Neelie Kroes [27] launching the European Cyber Security Month had a significant impact on the media coverage, the total number of Facebook 'likes' [28] and the number of followers of the ECSM Twitter account [29].

Details about how the six Facebook campaigns were set-up and related data can be found in the sections below.

5.1.4.1.1 EUROPE

EUROPE

COUNTRIES:

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

STATUS:

completed

DURATION:

3/9/2012–1/10/2012

NAME:

Join the EU CyberSecMonth

ADVERT:

October is the EU Cyber Security Month. Check out how to stay safe and secure online

TARGETING [30] :

98 580 420 users:

- who live in Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden or the United Kingdom;
- aged 18 and older,
- in one of the categories: science/technology, computer programming, small business owners, mobile (all), iPhone, RIM/Blackberry, Android, Windows Phone, others, iPad, active feature phone users or technology early adopters.

CAMPAIGN REACH [31]:

1 246 064

FREQUENCY [32]:

11.8

NUMBER OF IMPRESSIONS [33] :

7 507 532

NUMBER OF CLICKS [34]:

364 (pointing to http://www.enisa.europa.eu/activities/cert/security-month/pilots)

[26] http://www.enisa.europa.eu/activities/cert/security-month

[27] http://www.youtube.com/watch?v=7UwTAWrFpGI

[28] http://www.facebook.com/CyberSecMonth. As of 19 November 2012, the Facebook CyberSecMonth account has 65 Likes.

[29] https://twitter.com/CyberSecMonth. As of 19 November 2012, the Twitter CyberSecMonth account has 230 followers, 110 tweets and 61 following.

[30] The number of individual people who were targeted by this campaign.

[31] The number of individual people who saw sponsored stories or adverts in this campaign during the dates selected. This isdifferent to impressions, which includes people seeing them multiple times.

[32] The average number of times each person saw the ECSM campaign's sponsored stories or adverts

[33] The total number of times adverts have been shown on the site.

[34] The number of clicks this campaign's sponsored stories or adverts have received.

5.1.4.1.2 LUXEMBOURG

LUXEMBOURG

COUNTRY:

Luxembourg

STATUS:

completed

DURATION:

1/10/2012–13/10/2012

NAME:

Mois UE de Cybersécurité

ADVERT:

Découvrez toutes les activités locales et manifestations prévues à Luxembourg

TARGETING:

125 660 users

- who live in Luxembourg;
- aged 18 and older;
- in one of the categories: science/technology, computer programming, small business owners, technology early adopters, mobile users (all), smartphone/tablet users, feature phone users, Sony, LG, Motorola, HTC, Android (other), Samsung or Android (all).

CAMPAIGN REACH:

33 987

FREQUENCY:

19.9

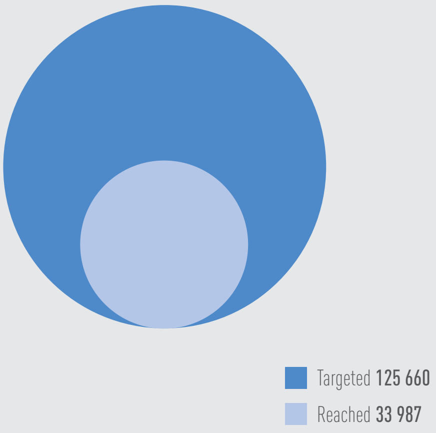
NUMBER OF IMPRESSIONS:

676 101

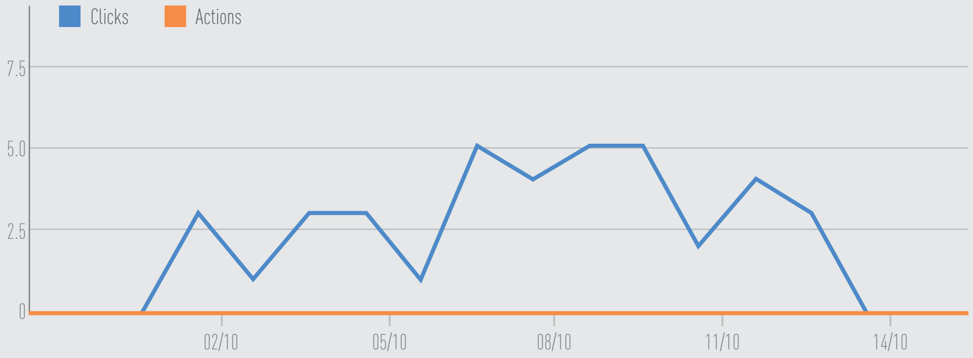
NUMBER OF CLICKS:

39 (pointing to http://www.enisa.europa.eu/activities/cert/security-month/pilots/luxembourg)

FIGURE 3: AUDIENCE OF LUXEMBOURG'S FACEBOOK CAMPAIGN



GRAPH 3: RESPONSE TO LUXEMBOURG'S FACEBOOK CAMPAIGN



5.1.4.1.3 NORWAY

NORWAY

COUNTRY:

Norway

STATUS:

completed

DURATION:

29/9/2012–26/10/2012

NAME:

Delta i EU-CyberSecMonth

ADVERT:

Se hvilke lokale aktiviteter og arrangement som er planlagt i Norge

TARGETING:

1 641 940 users

- who live in Norway;
- aged 18 and older;
- in one of the categories: science/technology, computer programming, small business owners, technology early adopters, mobile users (all), smartphone/tablet users, feature phone users, Sony, LG, Motorola, HTC, Android (other), Samsung or Android (all).

CAMPAIGN REACH:

27 476

FREQUENCY:

8.8

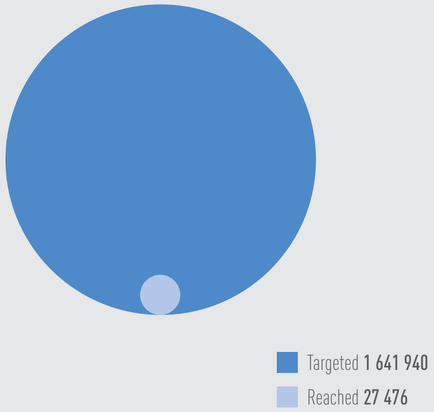
NUMBER OF IMPRESSIONS:

247 474

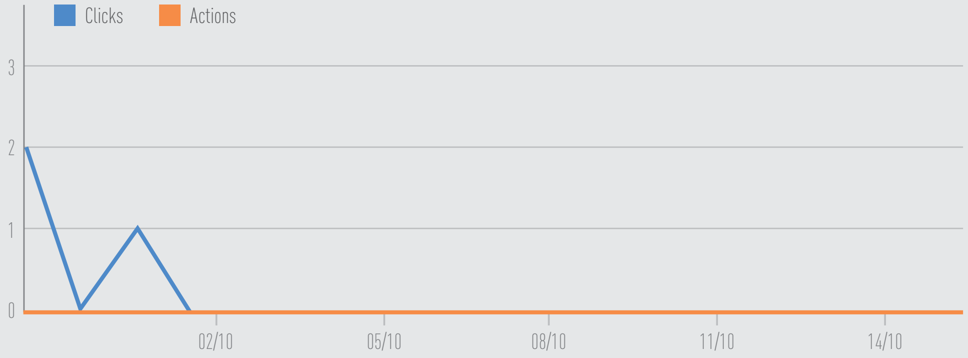
NUMBER OF CLICKS:

3 (pointing to http://www.enisa.europa.eu/activities/cert/security-month/pilots/norway)

FIGURE 4: AUDIENCE OF NORWAY'S FACEBOOK CAMPAIGN



GRAPH 4: RESPONSE TO NORWAY'S FACEBOOK CAMPAIGN



5.1.4.1.4 PORTUGAL

PORTUGAL

COUNTRY:

Portugal

STATUS:

completed

DURATION:

4/9/2012–2/10/2012

NAME:

Mês de Cibersegurança
Advert: Confira a variedade de actividades locais e eventos a serem realizados em Portugal

TARGETING:

1 452 440 users

- who live in Portugal;
- aged 18 and older;
- in one of the categories: computer programming, small business owners, mobile users (all), smartphone/tablet users, feature phone users, Sony, LG, Motorola, HTC, Android (other) or Samsung.

CAMPAIGN REACH:

184 746

FREQUENCY:

9.5

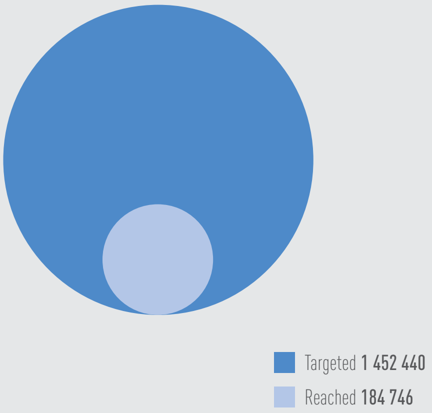
NUMBER OF IMPRESSIONS:

1 752 870

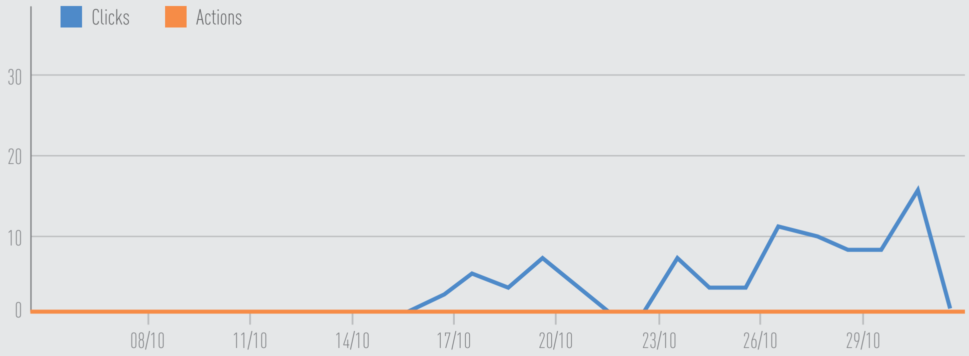
NUMBER OF CLICKS:

86 (pointing to http://www.enisa.europa.eu/activities/cert/security-month/pilots/portugal)

FIGURE 5: AUDIENCE OF PORTUGAL'S FACEBOOK CAMPAIGN



GRAPH 5: RESPONSE TO PORTUGAL'S FACEBOOK CAMPAIGN



5.1.4.1.5 SLOVENIA

SLOVENIA

COUNTRY:

Slovenia

STATUS:

completed

DURATION:

24/9/2012–5/10/2012

NAME:

EU mesec spletne varnosti

ADVERT:

Preveri lokalne dejavnosti in dogodke, ki se bodo odvijali v Sloveniji. Pridruži se nam!

TARGETING:

282 840 users

- who live in Slovenia;
- aged 18 and older;
- in one of the categories: science/technology, computer programming, small business owners, technology early adopters, mobile users (all), smartphone/tablet users, feature phone users, Sony, LG, Motorola, HTC, Android (other), Samsung or Android (all).

CAMPAIGN REACH:

99 005

FREQUENCY:

18.9

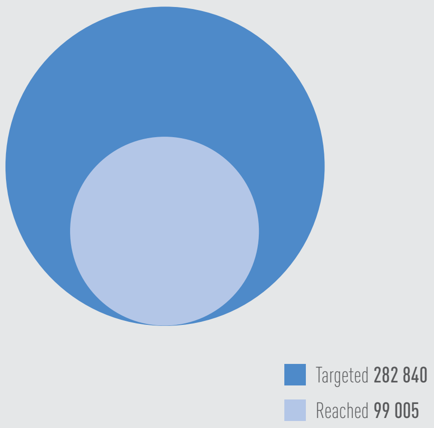
NUMBER OF IMPRESSIONS:

1 869 882

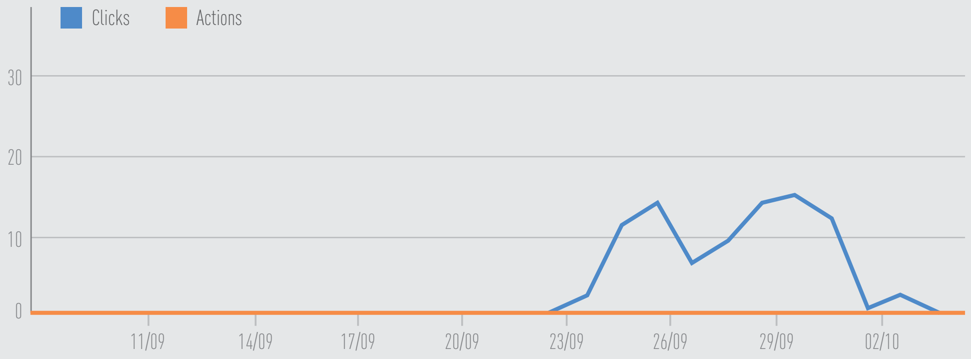
NUMBER OF CLICKS:

85 (pointing to http://www.enisa.europa.eu/activities/cert/security-month/pilots/slovenia)

FIGURE 6: AUDIENCE OF SLOVENIA'S FACEBOOK CAMPAIGN



GRAPH 6: RESPONSE TO SLOVENIA'S FACEBOOK CAMPAIGN



5.1.4.1.6 SPAIN

SPAIN

COUNTRY:
Spain

STATUS:
completed

DURATION:
10/9/2012–5/10/2012

NAME:
Mes seguridad cibernética

ADVERT:
Consulta todas las actividades que se celebrarán en España para el mes europeo de seguridad

TARGETING:
9 926 640 users

- who live in Spain;
- aged 18 and older;
- in one of the categories: science/technology, computer programming, small business owners, mobile (all), iPhone, RIM/Blackberry, Android, Windows Phone, others, iPad, active feature phone users or technology early adopters.

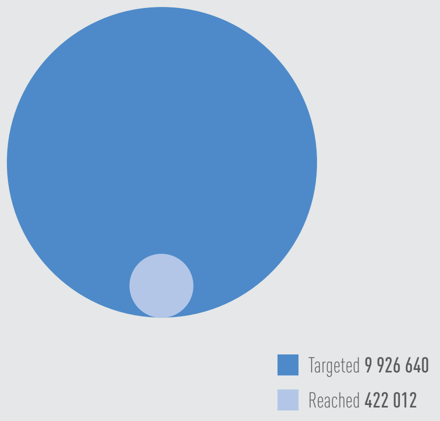
CAMPAIGN REACH:
422 012

FREQUENCY:
3.4

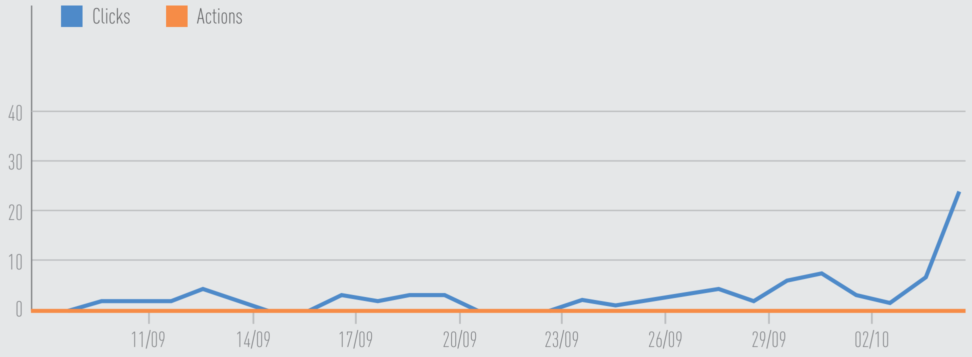
NUMBER OF IMPRESSIONS:
692 416

NUMBER OF CLICKS:
85 (pointing to http://www.enisa.europa.eu/activities/cert/security-month/pilots/spain)

FIGURE 7: AUDIENCE OF SPAIN'S FACEBOOK CAMPAIGN



GRAPH 7: RESPONSE TO SPAIN'S FACEBOOK CAMPAIGN



6 Lessons learned

The analysis of the data gathered throughout this report as well as the inputs received by the participating countries helped to identify a set of lessons learned. In addition, the experience of ENISA in its role of coordinator of the ECSM was key while performing this exercise. These lessons could be applied to future ECSMs.

- Better define the specific audience that is targeted by the awareness initiative in order to tailor the message content to the target group's knowledge or technical aptitude using the most effective communication channels.
- Produce all relevant material in at least all the official languages of participating countries.
- Make press releases available in at least all the official languages of participating countries.
- Produce video clips in different formats in order to allow their use for TV adverts.
- Make sure there are enough staff available during events. Particular attention should be paid to the number of staff available during weekends compared to weekdays.
- Produce giveaways according to the season of distribution (i.e. t-shirts distributed in cold weather did not appear to be a good idea).
- Involve an increased number of private companies to increase impact.
- Deal with changes in plans and keep interested parties informed.
- Ensure media coverage by planning possible interviews in advance. Be prepared for last-minute cancellations.

7 Conclusions

The data gathered and the analysis carried out led to the conclusion that the first ever European Cyber Security Month was a successful pilot project. The significant experience of the ECSM's participating countries and their commitment to achieving long-lasting change in human behaviour and perception of risks were the two key elements that led to a successful project.

The ECSM aimed at bringing citizens to reflect on the importance of being safe and secure online and raising awareness of NIS issues. Moreover, the pilot countries received benefits from this initiative by:

- including their national security events in a European initiative context;
- increasing their visibility at European level;
- improving positive public opinion about information security;
- increasing their efficiency in organising ECSM initiatives;leveraging existing material;
- sharing experiences and information with the other countries and ENISA.

Several elements ensured the success in the organisation of the ECSM:
- the Member States were fully engaged;
- intermediaries were involved in almost all countries;
- media coverage was significant both at European and at national level;
- the ECSM brand logo and associated values started to be recognised.

To conclude, ENISA believes that the 2012 European Cyber Security Month pilot project set the scene for the organisation of a fully fledged ECSM in the years to come.

European Network and Information Security Agency

BE AWARE, BE SECURE.
SYNTHESIS OF THE RESULTS OF THE FIRST EUROPEAN
CYBER SECURITY MONTH

Luxembourg: Publications Office of the European Union, 2012

ISBN 978-92-9204-063-5
doi: 10.2824/24665
Catalogue Number: TP-30-12-136-EN-N

TP-30-12-136-EN-N

enisa
European Network
and Information
Security Agency

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

Publications Office

ISBN 978-92-9204-063-5

doi: 10.2824/24665