



EUROPEAN  
CYBER  
SECURITY  
MONTH



# European Cyber Security Month 2016

## Deployment Report

DECEMBER 2016



## About ENISA

---

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

### Contact

For contacting the authors please use [ecsm@enisa.europa.eu](mailto:ecsm@enisa.europa.eu)

For media enquiries about this paper, please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu).

### Legal notice

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

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

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

### Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2016

Reproduction is authorised provided the source is acknowledged.

ISBN 978-92-9204-218-9, DOI 10.2824/984485

## Table of Contents

---

|                                       |           |
|---------------------------------------|-----------|
| <b>1. Executive Summary</b>           | <b>5</b>  |
| <b>2. Introduction</b>                | <b>7</b>  |
| <b>2.1 Scope and Objectives</b>       | <b>7</b>  |
| <b>2.2 Evaluation Methodology</b>     | <b>8</b>  |
| <b>2.3 Target Audience</b>            | <b>8</b>  |
| <b>3. Planning Phase</b>              | <b>9</b>  |
| <b>3.1 Coordination</b>               | <b>10</b> |
| <b>3.2 Marketing Material</b>         | <b>11</b> |
| <b>3.3 Partners</b>                   | <b>15</b> |
| <b>4. Execution phase</b>             | <b>16</b> |
| <b>4.1 Kick-off event</b>             | <b>16</b> |
| 4.1.1 Week 1                          | 17        |
| 4.1.2 Week 2                          | 17        |
| 4.1.3 Week 3                          | 17        |
| 4.1.4 Week 4                          | 17        |
| <b>4.2 National Campaigns</b>         | <b>18</b> |
| 4.2.1 France                          | 18        |
| 4.2.2 Germany                         | 18        |
| 4.2.3 Luxembourg                      | 19        |
| 4.2.4 Poland                          | 19        |
| 4.2.5 Slovenia                        | 20        |
| 4.2.6 Non-Country participation       | 20        |
| <b>4.3 Results</b>                    | <b>20</b> |
| <b>5. Evaluation</b>                  | <b>21</b> |
| <b>5.1 Questionnaire</b>              | <b>21</b> |
| 5.1.1 Results                         | 21        |
| 5.1.2 Conclusions                     | 24        |
| <b>5.2 Web analytics</b>              | <b>25</b> |
| 5.2.1 ECSM Web Page                   | 25        |
| 5.2.2 NIS Quiz                        | 26        |
| 5.2.3 ECSM Map of Activities          | 27        |
| 5.2.4 Social Media                    | 28        |
| 5.2.5 Media Reach                     | 30        |
| 5.2.6 Conclusions                     | 31        |
| <b>6. Conclusions and Future Work</b> | <b>32</b> |

|                 |  |           |
|-----------------|--|-----------|
| 6.1.1           | 2017 and beyond                                      | 33        |
| <b>Annex A:</b> | <b>Infographics by Country 2016</b>                  | <b>34</b> |
| <b>Annex B:</b> | <b>ECSM 2016 - Map of Partners Activities' Logos</b> | <b>44</b> |
| <b>Annex C:</b> | <b>Kick-Off Agenda</b>                               | <b>45</b> |

---

## 1. Executive Summary

---

For the fourth consecutive year, last October the European Cyber Security Month (ECSM) campaign took place across Europe. The campaign was supported by ENISA, the European Commission, Europol's EC3 and the European Banking Federation, plus partners from the Member States, the support for which propelled the campaigns success as measured by both the qualitative and quantitative data compiled. Although this year's campaign broke all previous growth records, the conclusions of this reports highlight a number of fundamental issues that need to be addressed in the coming years if the campaign is to reach its original objective which was to influence the security behaviour of citizens online. The weaknesses that have been highlighted, will be clarified and qualified in the coming year within the context of a campaign assessment. However within this report, recommendations are made to address these shortfalls in the near term.

The following recommendations have been put forward to mitigate these shortfalls:

- Draw up comprehensive communication plan with the assistance of the ENISA communications team and external expertise
- Populate the newly created website depository with partner material / information and seek ways to utilize this as an information hub for citizens
- Seek to create PPP's amongst partners and private companies that have demonstrated a willingness to work in awareness raising
- Build into the budgetary decision making process impact analysis that documents the perceived impact versus the cost, time and quality of budgetary decision.
- Re-focus the work plan on the goals and objectives of the campaign before considering which methodology to follow.

A crucial aspect of the evaluation was the extent to which the campaign addressed the overall objectives. A number of observations can be made regarding the impact towards some of these objectives such as the involvement of relevant stakeholders and the media's interest in Cyber Security which were indeed the case for both objectives. The other more crucial observation regarding the impact towards raising general awareness especially to the EU citizen, cannot be so easily made given the current data gathering methods used to evaluate the campaign.

Turning back to the objectives of European Cyber Security Month (ECSM), which 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. Each Member State decided upon the scope and how best to tackle these objectives given their experience and knowledge of the local community; and the number of activities and events it 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 access to the [cybersecuritymonth.eu](http://cybersecuritymonth.eu), posters, infographics and social media for participating countries to promote their activities.

This report provides an overview of the activities organised and presents a synthesis of findings on the basis of evaluation and performance information gathered via a questionnaire and media monitoring data.

The report is structured into three main parts: an introduction, the implementation phase and an evaluation of the campaign.

The introduction will provide readers with the policy context, scope and target audience of the campaign.

The implementation phase of the report highlights the mile stones that were achieved during the planning and execution phase of the campaign. This includes how events were organized and co-ordinated with partners, marketing materials used and insights into the execution of the campaign including results.

The final section of the report deals with the evaluation of the campaign, comparing this year's results with the previous year's and also provides input from the partners that was generated via a questionnaire; and finishes with a conclusion and outlook for the future.

## 2. Introduction

---

In early 2013 the EU published the “Cybersecurity Strategy of the European Union”<sup>1</sup> as a means to safeguard the online environment and providing the highest possible freedom and security, for the benefit of EU citizens. This strategy was jointly adopted by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy. It outlines the EU's vision in this domain, clarifies roles and responsibilities and proposes specific activities at EU level. Its goal is to ensure strong and effective protection and promotion of citizens' rights so as to make the EU's online environment the safest in the world.

End users play a crucial role in ensuring security of networks and information systems. In this context they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them. Several initiatives were developed in recent years. In particular, in October 2012, ENISA, with some Member States, piloted the "European Cyber Security Month" campaign.

In the context of the ECSM project, the Commission invited the Member States to organise a yearly cybersecurity month with the support of ENISA and the involvement of the private sector, with the goal to raise awareness among end users. ECSM and the private sector were also encouraged to join efforts in order to promote cybersecurity awareness at all levels, both in business practices and in the interface with customers.

ECSM runs for the entire month of October, with ENISA publishing new material and focusing on a different topic each week. Along with ENISA, various stakeholders, ranging from the private sector, education, the European Commission (EC) and other EU bodies, join together in a common vision by organising activities with special focus on training, strategy summits, online quizzes and provide general presentations to end users toward the establishment of an EU cyber-security culture.

This report summarises the activities carried out by ENISA and its partners for this year's ECSM campaign and presents the evaluation results and conclusions. More importantly, it seeks to trigger a discussion among partners with respect to improvements that can be made for ECSM to strategically achieving its objectives in the future.

### 2.1 Scope and Objectives

The scope of this evaluation includes all the campaigns activities and their impact within 2016, comparing the results with those of 2015, and also measuring the extent by which these activities addressed the campaign's objectives.

The main objectives of the campaign were as follows:

- 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;

---

<sup>1</sup> <https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace>

- to enhance attention and interest with regard to information security through political and media coordination.

The evaluation results and estimated impact of the ECSM activities shall allow us to discuss lessons learned deriving from this exercise and shall help us to draw attention to related issues, hence acquiring a broader view for further enhancing the ECSM's development and effectiveness.

In addition, among other aims, analysis 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 will be in need to face up to a similar challenge, namely how to engage citizens to change their information security behaviour.

## 2.2 Evaluation Methodology

ENISA gathered information with regards the organization and achievements of the campaign using two distinct methods:

1. by feedback from ECSM partners given a Q&A questionnaire, and
2. by the use of media monitoring services to gather analytical data.

The questionnaire aimed at extracting pertinent information on the overall impact of the campaign based on partners' feedback with respect to ENISA's supportive role. More specifically, some of the elements assessed involve the level of support and its usefulness provided to partners, the impact of promotion material used and marketing strategies followed, future engagement with the private sector or other international campaigns, etc.

The data gathered by the media monitoring service was aggregated by combining data elements from different sources to provide insights and identify the effectiveness of the messages, media channels and the campaign as a whole in reaching the general population.

## 2.3 Target Audience

This evaluation 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 professionals and other target groups who attended events and conferences organised across Europe during the month of October 2016.

### 3. Planning Phase

---

ENISA supported the organisation of the European Cyber Security Month campaign in various ways, such as:

- coordinator of the organisation of the ECSM;
- hub for all participating countries;
- collector of available material and generator of synergies between 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 (posters and infographics).

The Agency coordinated the organisation of the ECSM campaign, by means of becoming a “hub” for all participating countries and providing suggestions, replying to enquiries and generating synergies between countries when possible.

ENISA provided guidance and expertise by organizing a monthly conference call with all partners so as to seek synergies, collaboration and guide the campaign. The common message of “Cyber Security is a Shared Responsibility” was promoted among Member States and material was provided to help with their cyber security education and awareness campaigns. 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;
- posters and infographics<sup>2</sup>;
- social media web banners<sup>3</sup>;
- video clips<sup>4</sup>;
- NIS Quiz<sup>5</sup>.

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

The planning phase of the campaign started in earnest with a request to partners from previous year’s campaign to join the monthly conference calls.

The graph below depicts the mile stones of the planning phase leading up to October and also the execution phase. It highlights key events, meetings, conference and phases of the campaign.

---

<sup>2</sup> <https://cybersecuritymonth.eu/press-campaign-toolbox/material>

<sup>3</sup> <https://cybersecuritymonth.eu/press-campaign-toolbox/visual-identity>

<sup>4</sup> <https://www.youtube.com/watch?v=Rr-gVUG9koM>

<sup>5</sup> <https://cybersecuritymonth.eu/references/quiz-demonstration/intro>

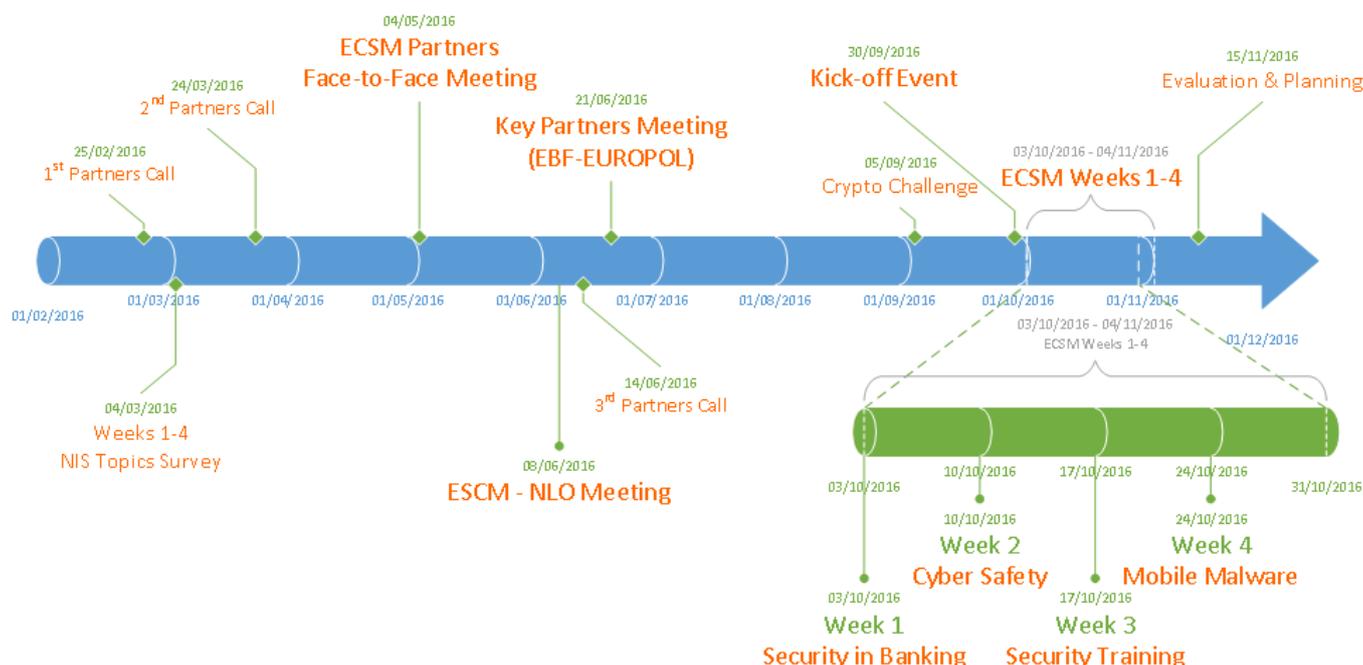


Figure 1: ECSM timeline of events planning

### 3.1 Coordination

#### 3.1.1.1 Conference Calls and Meetings

Monthly conference calls with partners were scheduled in order to update partners on the plans, get feedback and hear from partners on their national campaign plans. These calls provided opportunities for partners to seek synergies and form collaborations. Minutes were drawn up by ENISA after every call, including a list of action points and after approval from the Head of Unit they were distributed to the conference call participants. As expected the participation rate increased as the campaign month drew near with an average of 10 to 15 participants on the call at a time.

During the year a number of face to face meetings were held with partners in order to finalize key areas of the campaign such as the themes of the month and the organization and logistics of the kick-off event. These were held at partner offices in Brussels and in ENISA offices in Athens.

#### 3.1.1.2 Themes of the Month Survey

A survey was launched amongst the partners to determine which would be the four themes of the month, one theme for each of the weeks in October.

ENISA suggested twelve possible themes for the partners to choose from and with the help of the partners throughout regular meetings and discussions, these themes were eventually narrowed down to the four most prominent as shown below:

1st week – October 3-7: Cyber Security in Banking – supported by the European Banking Federation

2nd week – October 10-14: Cyber Training

3rd week – October 17-21: Cyber Safety

4th week – October 24-28: Mobile Malware – supported by Europol EC3

### 3.1.1.3 Kick-Off Event

Collaboration was forged early in the year with the European Banking Federation, who approached ENISA requesting to host the kick-off event at their premises in Brussels but also to promote various activities with respect to the first theme-week of October, that of Security in Banking. On the other hand Europol EC3 was engaged into promoting the fourth theme of the month directly related to secure practices with mobile devices. These collaborations were well received by the ECSM partners during the monthly conference calls, and plans were put in motion to organize the event. Three face to face meetings were eventually held between key partners for the organizational details of the kick-off event.

Responsibilities for the arrangements of the communications and the logistics for the event were determined early on, with two documents being drawn up, the “Common Communication Strategy” and the “Script” of activities for the kick-off event. The former document aimed at aligning the partner’s messages and press releases on the day of the event, while the latter provided a detailed outline of how the event would pan out in real time including roles, responsibilities and contact points.

Policy makers, industry experts and representatives from competent authorities were invited to attend the launch and had been encouraged to come forward as speakers or panellists for either of the four sessions on the weekly themes, including:

- Security in banking
- Cyber security training
- Cyber safety (*child extortion, cyber bullying & IOT*)
- Mobile malware

Furthermore, in practice the planning phase consisted of an extensive consultation with stakeholders like the Commission, NLO network, and international partners in order to come up with a consolidated version that anyone could easily follow. Regarding the management of the communication process, all feedback, issues and ideas were tackled in a tailored manner to fit the needs and purposes of organisations involved.

## 3.2 Marketing Material

A series of activities were planned to market the European Cyber Security Month project. The following sub categories identify the various marketing solutions of the campaign.

### 3.2.1.1 Visual identity

To strengthen visibility and public recognition of the European Cyber Security Month, ENISA created some years ago a visual identity including a logo<sup>6</sup>, 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 and the logo was used by partners on their material, videos and social media to link their efforts up to the European campaign.

### 3.2.1.2 Slogan

The slogan 'Cyber Security is a Shared Responsibility' was created to give the project an identity and a positive image. It has been used in this year's campaign and included with posters, infographics and the cybersecuritymonth.eu website. The slogan was also promoted for use by the member states that organized their local activities and at ENISA's press releases.

### 3.2.1.3 Press releases

The European Cyber Security Month featured a diverse range of activities and events, and as part of the build-up ENISA launched press releases<sup>7</sup> that aimed to bring anticipation to the launch of the campaign.

### 3.2.1.4 Social media - banners

The dedicated social media accounts of Twitter and Facebook were used as a medium for disseminating 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 campaign and assisted in engaging the digital citizen.



Figure 2: ECSM 2016 facebook banner.

### 3.2.1.5 Poster and Infographics

An ECSM 2016 poster<sup>8</sup> was created to highlight the four themes of the month, the kick-off event and the overall message that this is a European wide effort with a single underlying message. A number of partner member states participated in the creation of a dedicated country infographics. Each country infographic highlighted the key information and data regarding their campaigns and achievements. A total of 10 countries participated in creating an infographic. Finally ENISA created a single unified infographic of the achievements of this year's campaign.

---

<sup>6</sup> <https://cybersecuritymonth.eu/press-campaign-toolbox/visual-identity>

<sup>7</sup> <https://www.enisa.europa.eu/news/enisa-news/a-week-to-go-for-the-european-cyber-security-month-launch-1>

<sup>8</sup> <https://cybersecuritymonth.eu/press-campaign-toolbox/material>



Figure 3: ECSM poster and infographics by country (left-to-right).

### 3.2.1.6 Videos

Two videos were produced for this year’s campaign. The first was a short animated video<sup>9</sup> describing the objectives of the ECSM campaign, highlighting the scope and target audience. The other video<sup>10</sup> was of interviews taken of speakers during the kick-off event on the 30th September in Brussels. Both videos will be used to further promote the campaign amongst citizens and organizations.



Figure 4: ECSM Animated Video Snapshot.

<sup>9</sup> <https://www.youtube.com/watch?v=Rr-gVUG9koM&t=2s>

<sup>10</sup> <https://cybersecuritymonth.eu/press-campaign-toolbox/material>

### 3.2.1.7 Website

The ECSM website<sup>11</sup> was re-organized at the beginning of the year and the home page was given a facelift. Changes took into consideration websites of similar awareness raising campaigns, which included the addition of a countdown clock leading up to the 1<sup>st</sup> October and more user friendly navigation to the relevant areas. A dedicated partner page was introduced to display the names and contact details of the organizations that are lead collaborators of the campaign.



Figure 5: Map of activities across Europe

### 3.2.1.8 NIS Quiz

The NIS quiz<sup>12</sup> was updated this year so that it would better reflect the new GDPR and other regulatory & legislative changes in NIS. Another important feature of quiz was the translation into the 23 official languages of the EU, now making it accessible across Europe to all EU citizens.

<sup>11</sup> <https://cybersecuritymonth.eu/>

<sup>12</sup> <https://cybersecuritymonth.eu/references/quiz-demonstration/intro>



Test your e-skills and obtain a CyberSecMonth badge by filling in this quiz. Try it!

Please choose one of the two topics below

 Privacy       General Security

Please choose which level you would like to start with:

Level 1(starter)  
 Level 2(advanced)

Please choose a language

English

**BEGIN THE QUIZ**

Figure 6: NIS quiz upgraded and now supported in 23 EU languages

### 3.3 Partners

The National Liaison Officers network were contacted in order to identify the national contact point responsible for the awareness campaign in their country.

The following list of organizations / institutions were fully engaged partners in this year's campaign.

- Federal Chancellery of Austria
  - CERT-EE Estonia
  - National Cyber Security Centre Finland (NCSC-FI)
  - National Cybersecurity Agency of France (ANSSI)
  - Federal Office for Information Security Germany (BSI)
  - National Safer Internet Centre Czech Republic (NCBI)
  - National Cyber Security Centre Hungary (NCSC)
  - Cyberworld Awareness and Security Enhancement Services Luxembourg (CASES)
  - Research & Academic Computer Network Poland (NASK)
  - CERT-RO Romania
  - Norwegian Centre for Information Security (NorSIS)
  - Platform for the Information Society Netherlands (ECP)
  - SI-CERT Slovenia
  - CERT Slovakia
- 
- European Banking Federation (EBF)
  - Europol EC3
  - Confederation of European Computer Users Associations (CECUA)
  - ECDL Foundation

## 4. Execution phase

---

### 4.1 Kick-off event

The execution of the kick-off event rested heavily on the preparation work that was put in place during the preceding months between ENISA, EBF and Europol EC3. Clear lines of responsibility were drawn up early on during the planning phase; and the communications between the three organizations were further strengthened by three face to face meetings leading up to October. The kick-off event was a half day event that consisted of four sessions the details of which are presented below.

The opening speeches for the kick-off event consisted of introductions from the following speakers:

- Sébastien De Brouwer, Executive Director, EBF
- Wim Mijs, Chief Executive, EBF
- Steve Purser, Head of Core Operations, ENISA
- Olivier Burgersdijk, Integrated Data Management, Europol
- Ken Ducatel, Director, DIGIT

A session regarding “national cyber security month campaigns” and another session focusing on “cyber awareness” were the responsibility of ENISA to organize. Five ECSM partners volunteered to present their campaigns which consisted of the following panellists:

- France: Anne-Charlotte Brou from Agence nationale de la sécurité des systèmes d’information (ANSSI),
- Germany: Hanna Heuer from Federal Office for Information Security (BSI),
- Luxembourg: Daniele Bisdorff from Ministère de l’économie du Luxembourg (CASES),
- Netherlands: Marjolijn Durinck from Platform voor de Informatiesamenleving (ECP),
- Norway: Peggy Heie from Norsk senter for informasjonssikring (NorSIS).

The session on Cyber Awareness consisted of the following panellists:

- Moderator: Jakub Boratynski, Head of Cybersecurity and Digital Privacy, DG CNECT
- Dr. Veronica Donoso, Executive Director, INHOPE
- Dr. Hans Martens, Insafe network coordinator, European Schoolnet
- Erka Koivunen, Cyber Security Advisor, F-Secure Corporation
- William O’Connell, Chief Business Security Officer, ADP

The other sessions during the kick-off event were organized by the European Banking Federation and Europol’s EC3 respectively, one focusing on Security in Banking and the other on Mobile Malware.

Security in Banking session consisted of the following panellists:

- Moderator: Keith Gross, Chair EBF, Cyber Security WG
- Wien De Geyter, Secretary General, Febelfin
- Troëls Oerting, Group Chief Information Security Officer, Barclays

- Koen Hermans, Public Prosecutor, Eurojust
- Peter, Kerstens, Advisor for Financial Sector Cybersecurity, DG FISMA

Mobile Malware session consisted of the following panellists:

- Moderator: Olivier Burgersdijk, Integrated Data Management, Europol
- Michael Shaulov, Head of Go To Market, Mobile Security, Check Point Software Technologies
- Senan Moloney, VP Cyber Threat Intelligence, Barclays
- Tomislav Vazdar, Chief Security Officer & Head of Corporate Security, Erste & Steiermärkische bank
- Daniel Lawrence, Detective Inspector, NPCC National Cyber Crime PROTECT Coordinator, CERT UK

All the sessions proved informative and generated much discussion amongst the audience. ENISA received positive feedback from the audience and the majority of the participants remained until the closing remarks of the event.

The communication unit of ENISA prepared a press release for the day of the kick-off event in collaboration with the European Commission; that was distributed to the other key partners of the campaign for feedback before release. Moreover, a weekly news item was prepared by the communication unit and released on the ENISA website to inform readers of the upcoming activities in the beginning of each of the weeks.

#### **4.1.1 Week 1**

The first week kicked off with an online ask me anything “AMA” session via the website Reddit. On the 4<sup>th</sup> October ENISA and F-Secure received questions from citizens related to Cyber Security. The session lasted over 2 hours and received 486 comments, was up-ticked to the home page of Reddit that has over 13 million subscribers and received just under four thousand points.

#### **4.1.2 Week 2**

During week two of the campaign ENISA made two significant releases, foremost was the release of the updated version of the NIS Quiz which was now also available for the first time in 23 official languages of the EU. The second release of the week was the official ECSM animation video. This is a 2 minute video that introduces the viewer to ECSM and explains the what, where, how and who of the campaign.

#### **4.1.3 Week 3**

A conference at the University Piraeus was organized with ENISA and the university for the purposes of educating undergraduate students of Informatics and Information Technology at the university. Presentations were given by the Ionian University, the Cyber Crime Unit of the Greek police and the Hellenic Authority for Communication Security and Privacy.

#### **4.1.4 Week 4**

The mobile malware theme for the month was organized by Europol EC3 and a number of participating countries with the lead country being the Cyber Crime unit of the Greek Police. For this reason on the 25<sup>th</sup> October ENISA arranged a closed workshop for police officers at the Police HQ. This was a half day morning session that included a live demonstration by ENISA.

## 4.2 National Campaigns

The following section provides readers with insight into some of the national campaigns that were organized by ECSM partners. The feedback was gathered by ENISA using a questionnaire that was distributed to the partners at the end of the campaign.

### 4.2.1 France

European Cybersecurity month (ECSM) was a great opportunity to give more visibility to good practices that ANSSI has developed, to work with partners and use various communication material. For this edition, ANSSI focused on promoting the good practices already promoted by our technical recommendations, guides and online interactions. It is the first year that ANSSI was participating actively in the campaign so the main idea was to give more visibility to our daily actions to raise awareness about cybersecurity. For instance, more than 17 events were organized by ANSSI agents, directed to students, administrations as well as private companies.

ANSSI's main security recommendations were our "12 rules" guide book reminding the importance of a good password and regular updates. ANSSI also took this opportunity to build new partnerships in France, with the government, the CNIL and public administrations (Europol France, gendarmerie), as well as to strengthen international partnerships with the BSI.

ANSSI also initiated contact with the private sector – regarding a possible future collaboration. For instance, ANSSI were able to build exchanges online, through Twitter, with the BSI linking their glossary project designed for the ECSM with ANSSI's French glossary. The kick-off event in Brussels was a great opportunity to exchanges the national coordinators' point of view and organization of this event in their respective countries.

Regarding ECSM in France, the events had been successful and new inquiries were made to build cooperation for the next edition.

### 4.2.2 Germany

As national coordinator in Germany, the BSI supported the ECSM especially with activities for private users. Based on the weekly topics of ENISA the BSI provided information & material such as: animated videos, which where we explaining risks and preventive measures, distributed via our social media channels and BSI website for private users, further information regarding the topics on our website, and a press release on each topic.

Furthermore, the BSI produced two radio features and set up a cyber-security ABC on facebook, where we explained different terms. The BSI also took the ECSM as an opportunity to invite representatives of think tanks, NGOs, ministries and journalists to a discussion on cyber security and its societal implications. Additionally, BSI ran activities with partners, e.g. support a webinar on basic protection held by klicksafe and started an online-survey in close cooperation with the police crime prevention on the behaviour of private users regarding security on the internet and on their experiences with cybercrime. For SME the BSI produced a flyer with some security recommendations on different aspects of cyber security.

To raise the visibility of the ECSM in Germany the BSI set up a project office which tasks were to contact possible partners, provide them with information and give ideas on possible activities. The project office will continue its work throughout the year. With the support of the project office the BSI won more than 70 partners in Germany who established more than 120 activities around October. The range of activities was quite wide, from webinars and social media activities to live-hacking events and a whole thematic day with workshops, discussions and so on.

Overall, the BSI was satisfied with the results of this years ECSM campaign in Germany. BSI was able to reach more partners and by this possibly more people and to get them involved in cyber security. The press releases were published in different media, especially in newspapers. The videos had each a few thousand views on social media and our website. The cyber security-ABC (27 postings) had an average outreach of 3.500 views on facebook. The radio features had an outreach of 3.000.000 listeners (data provided by the stations). More than 1.600 people participated in the online-survey.

#### 4.2.3 Luxembourg

The local ECSM coordination was done by the ministry of the Economy, directorate for electronic commerce and information security. Promotion and organization of the events was granted by SECURITYMADEIN.LU, the main national online portal for cybersecurity.

ECSM campaign was rolled through a series of 10 events, (approx. 1,000 people in total). 5 events were dedicated to cybersecurity for SMES', local and international experts as well as cybersecurity start-ups; 3 were focused on raising awareness among youth and the elderly; 2 presented cyber-risks to Luxembourg consumers.

The Luxembourg secretary of state of the Economy appeared at 2 occasions, highlighting the importance of cybersecurity for Luxembourg and welcoming the ECSM initiative.

Major events were the "Cybersecurity4success" conference and workshop day for SME's taking place at the Luxembourg Chamber of Commerce, as well as the "Cyber security day" organized with PriceWaterhouseCoopers (PwC). Other local events included a "crypto party" for kids, an "information day" for seniors, a presentation to Luxembourg consumers. Furthermore ECSM logo is part of the BEE SECURE 1 year campaign "Share Respect", gathering 18 national partners and associations and being mainly displayed in schools and public spaces from October 2016 to sept 2017. This years' edition was proud to count on a partnership with Luxembourg Law enforcement, Luxembourg Banking Association, and national youth initiative for the dissemination of the Europol's Mobile malware campaign.

Partners of the October month activities included: Maison de l'Europe, the Chamber of Commerce, Europe Enterprise Network, House of Training, PwC; The secretariat of the Benelux Union; Union luxembourgeoise des consommateurs. Partners specifically dedicated to the Europol Mobile Malware campaign were: ABBL, Luxembourg Bankers Association; The National Police and BEE SECURE, governmental initiative raising awareness among young people and public at large.

Online promotion was done through 4 main partner websites with approx. 1,000 unique visitors for the month. 5 press releases were sent; 15 website news were released. Over 20.000 people were reached through Facebook.

The impact of the BEE SECURE campaign cannot be analyzed yet as it continue into 2017 (30.000 flyers and 3300 posters are being distributed; 72 trainings will take place in Luxembourg schools.

#### 4.2.4 Poland

NASK organised 5 major activities, and was engaged in preparation and promotion of Europol materials. Some of the activities were still ongoing into the later end of 2016. The following are some stats for the campaign in Poland during October. Secure: 500 participants capture the flag; 704 unique visitors visited the main page of the project, 141 started the competition, and there were 9 correct solutions (3 fastest users were rewarded)

Quizzes: 385 participants What to do if... educational materials: <100 visits  
Bezpiecznymiesiac.pl: 2932 unique users, Facebook reach 151, Twitter impressions: 3640

#### 4.2.5 Slovenia

For ECSM 2016 CERT Slovenia held a press conference addressing frauds when shopping online. CERT SL dealt with a lot of cases, where people lose more than a few thousand EUR shopping online and stumbling upon fake sellers. CERT SL invited all the major public agencies and inspectorates in Slovenia to speak about this issue with the public.

CERT SL prepared online quiz with 8 questions about most common online frauds and security issues. The quiz was completed 6000 times, 1400 users agreed to sign up to the mailing list within the quiz, which was one of the main goal: to gain contacts for further work. Besides the quiz CERT SL prepared 4 videos which addressed the 4 most common frauds; sextortion, fake shops, ransomware and Airbnb frauds. Videos were played on Youtube and Facebook. They reached 120.000 views on YT and had almost 3 million reach on Facebook. Which means that not a single Slovenian FB user could avoid the message; frauds do happen however CERT SL are here to help.

All of CERT SL described activities were supported with press releases and media coverage that were well received. Through month there were more than 40 media mentions. Including those in talk shows (they invited CERT SL as guests), CERT SL were guests at news on national TV and commercial TV's. CERT SL prepared statements for radio shows and received more than 30 media mentions in printed newspapers and news portals. This was another key goal; to reach audience and users that don't use social media and Youtube often.

#### 4.2.6 Non-Country participation

CECUA (Confederation of European Computer User Associations, see [www.cecua.eu](http://www.cecua.eu)). The 2016 campaign was the second year in a row that CECUA joined the group of partners for ECSM. Security is high on the CECUA Agenda as technology can provide security solutions however in the end it is the awareness of people which counts. For ECSM 2016 CECUA produced publications for the European and national level and used further communication channels to raise awareness.

### 4.3 Results

Highlights of 2016 campaign:

1. 455 activities encoded in the official calendar from public and private stakeholders
2. 32 countries with events taking place in October
3. 120 participants at the ECSM kick-off, oversubscribed with over 160 participants registered
4. 429 articles published in October referring to ECSM
5. 465 courses registered in 28 countries for the NIS Education map
6. 14,239 visits to the for [www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) site in October
7. 57,890 page views to the for [www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) site in October

## 5. Evaluation

---

The indicators used to evaluate the campaign demonstrated a significant increase in visibility from previous years. Be they the number of activities registered on the ECSM website, the number of visitors to the website or the number of followers on twitter, for which the percentage change this year compared to the previous three years was above average across the board.

The distribution of media reach and articles peaked at two points during the campaign, initially during the launch of the campaign on the 30<sup>th</sup> September which was to be expected given the media push by all three key partners during the kick-off event; the second point was on the 24<sup>th</sup> October at the beginning of the final week of the campaign with the start of the Mobile Malware theme, that was coordinated and organized by Europol EC3.

Another measure of the success of the campaign was the participation rate of the kick-off event that was oversubscribed with over 160 participants registered the day before the event, with finally 120 participants turning up on the day, which was the capacity of the venue. This contrasts greatly with the amount of participants in the previous year's kick-off event that was half the number of participants of 2016.

Turning to the objectives of the campaign as described in section 2.1 above and assessing the results in this context, we can make the following concrete observations:

- Relevant stakeholders were involved in the campaign such as the EBF and Europol EC3
- Media interest did increase as measured by the number of articles published during October
- Attention to information security through political and media coordination was enhanced as a result of the high level representation during the kick-off event

What is less concrete to determine is the campaigns impact at raising general awareness about NIS and promoting safer use of internet for all users. This is because the analytical information that is currently being gathered to evaluate the campaign does not provide for this level of granularity and the resources required for such a study to be conducted are beyond the resources allocated for this project.

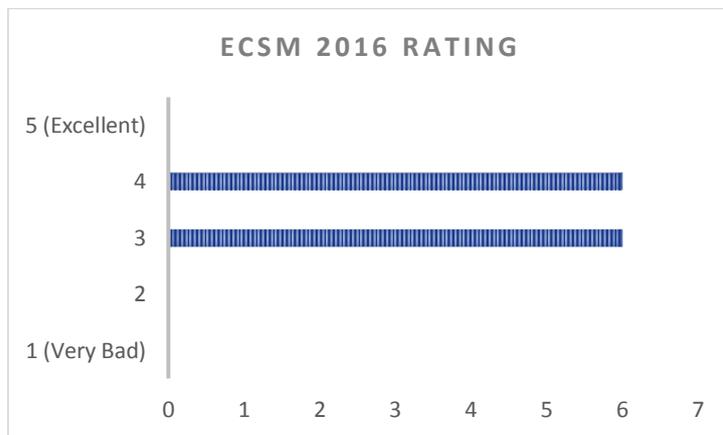
### 5.1 Questionnaire

The questionnaire is an important tool to help measure the impact of the campaign from the point of view of the partners that were engaged in the campaign. The charts below present the replies of 12 partners in contrast to 24 that participated in the previous year, a substantial decrease that was unexpected given the results of all the other indicators.

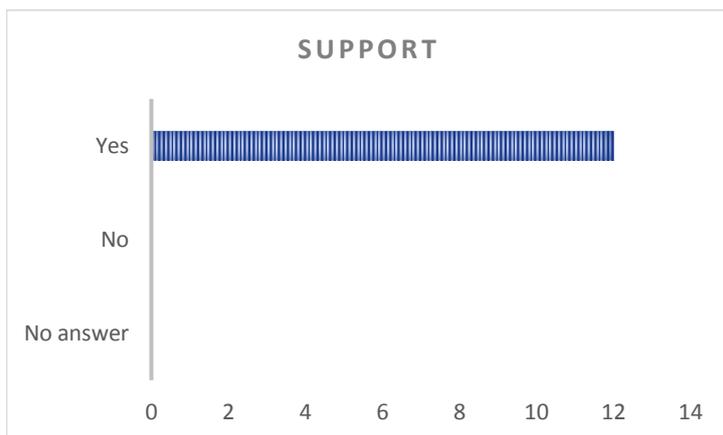
#### 5.1.1 Results

The questions of the survey and the results including feedback from partners are presented herein:

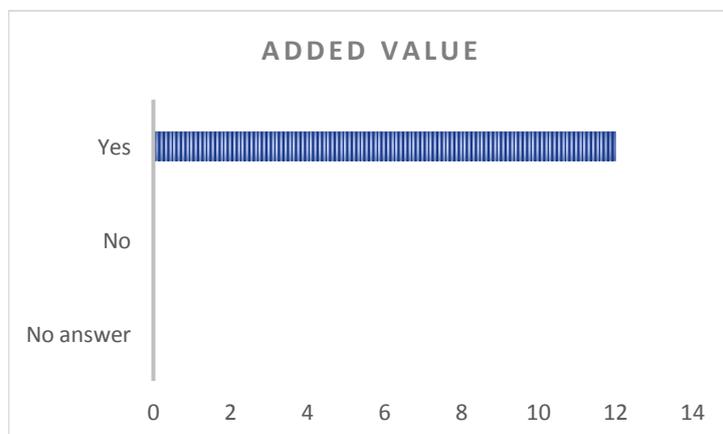
1. How would you rate the overall implementation of the ECSM 2016 campaign (scale 1-5)?



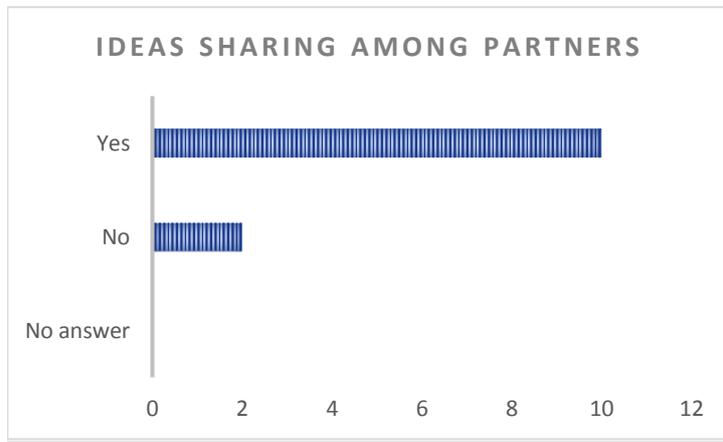
2. Did ECSM support in a satisfactory manner the outreach and promotion of your work?



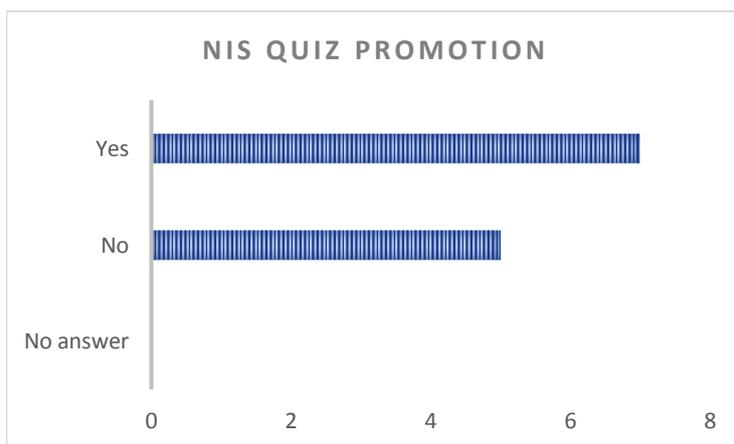
3. Did ECSM add value to your national campaign?



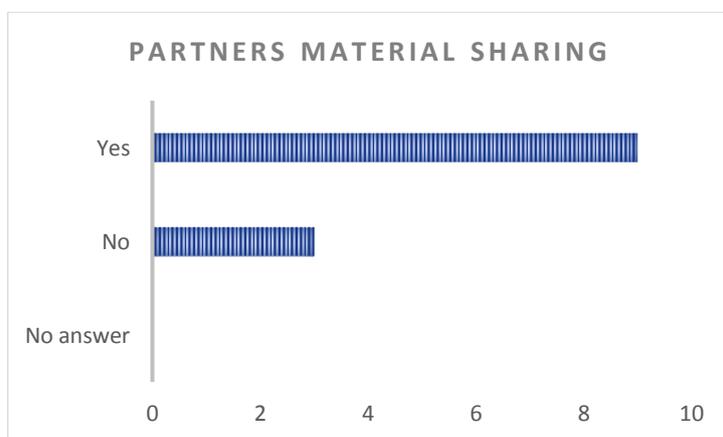
4. Do you think the campaign succeeded in the sharing and promotion of new ideas among ECSM partners?



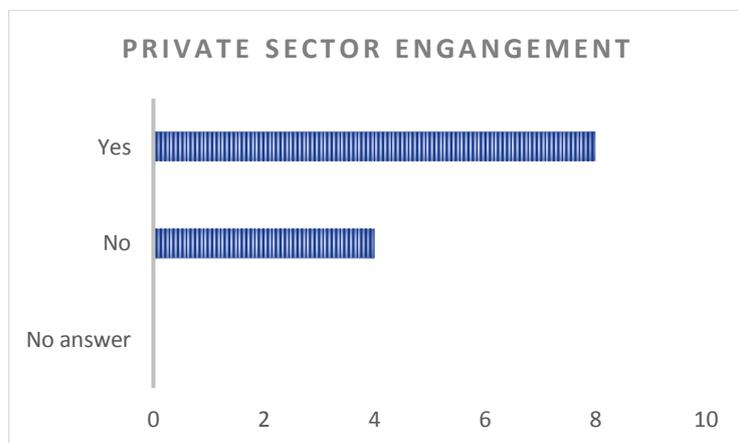
5. Do you think the NIS Quiz should be better promoted?



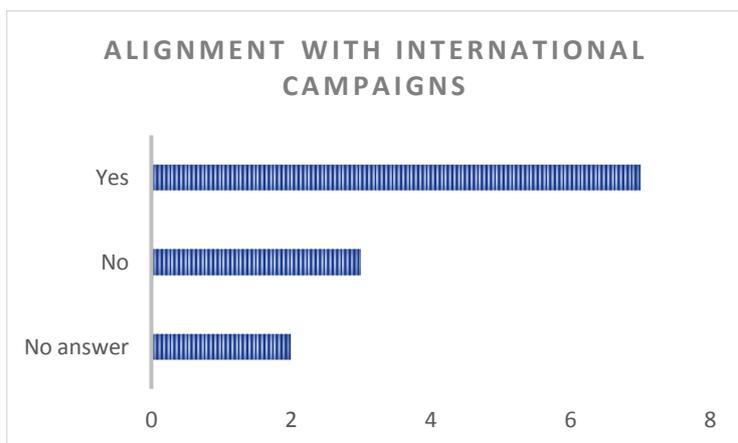
6. Could ECSM better promote the material produced by its partners' campaigns?



7. Would you want ENISA to facilitate in the engagement of the private sector in future campaigns?



8. Would you want to further align ECSM with international awareness raising campaigns?



### 5.1.2 Conclusions

All the partners rated ECSM campaign with a score of 3 or 4 out of 5 (Question 1). There were no answers provided from partners scoring the campaign in a negative way (scores 1 or 2). However, there were no answers giving an excellent score, which could be a signal that there is still space for improvement in the minds of the partners.

The overwhelming majority of partners stated that the campaign added value toward their national campaigns and that it provided the support they needed and required for sharing ideas (Questions 2, 3 and 4). Nevertheless, partners emphasised the need for greater effort in promoting the material produced by them at the national level (Question 6). This means that essential outputs in cyber security awareness raising remain isolated or hidden at

national level, hence preventing their dissemination among partners across the EU and eventually down to the EU citizen. This feedback has been noted and plans have already been put in place to address this issue early in 2017.

Some of the proposed solutions received from partners for the sharing of material include:

- Including in the ECSM website a new feed of partner related articles and news related to the materials they produce and pointing back to their work,
- Informing partners of material produced by other partners by email or other means,
- Partners to share social media posts regarding ECSM material,
- Produce a timeline of the partner's campaigns with their outputs,
- Create a depository of such material (with selected translations) at the ECSM website.

Further efforts to promote NIS Quiz was also emphasized by the partners (Question 5). This feedback reflects the lack of communication and marketing by ENISA after the release of the updated version of the quiz and its availability into all the official languages of the EU. Other proposals included the use of the NIS quiz in national campaigns and their websites, possibly by advertising a pointer to the original site of ECSM but also better management of social media platforms to increase visibility.

With regard to ENISA facilitating the private sector's engagement in future ECSM campaigns (Question 7), the majority of answers seem to favour such an approach. In this context, "pros" and "cons" of such an approach were provided as feedback. Positive considerations of such a collaboration included: the better outreach of the ECSM campaign and the willingness of the private sector to collaborate at the national level will enhance partners' awareness raising campaigns. On the other hand certain concerns were expressed such as: private sector runs its own marketing agenda and will not engage in producing awareness raising related material and that ECSM may be seen as a commercial opportunity, and finally; having a clear understanding and control over the roles activities may require additional effort.

The overall perspective of aligning ECSM with other international campaigns was positive, as long as the scope and objectives are shared (Question 8). On the other hand, reasonable scepticism was expressed on the strategic approach that should be followed in this case and that such an approach should be clearly defined.

## 5.2 Web analytics

Web analytics provided the statistical data for ECSM web site and social media channels. The purpose of gathering these figures were to evaluate the impact and visibility of the campaign.

### 5.2.1 ECSM Web Page

The analysis takes into consideration multiple variables in relation to different types of access points to the ECSM website in the period of October.

Statistics for October include:

- ECSM page views: 57,890.
- Users accessing the website: 14,239.

- Total Sessions: 18,490.



Figure 7: Graph overview of ECSM web site sessions.

The “pie” chart on the right hand side of Figure 7 shows the percentage of new visitors accessing the ECSM web page only once with those revisiting the web page multiple times. While this is encouraging, ENISA recognises the need of finding the means of keeping the interest of users “alive” for a greater period of time.

Below is a comparison between this year’s campaign and previous years with respect to the number of sessions and page views to the ECSM webpage, where there exists a stable almost linear increase in popularity.

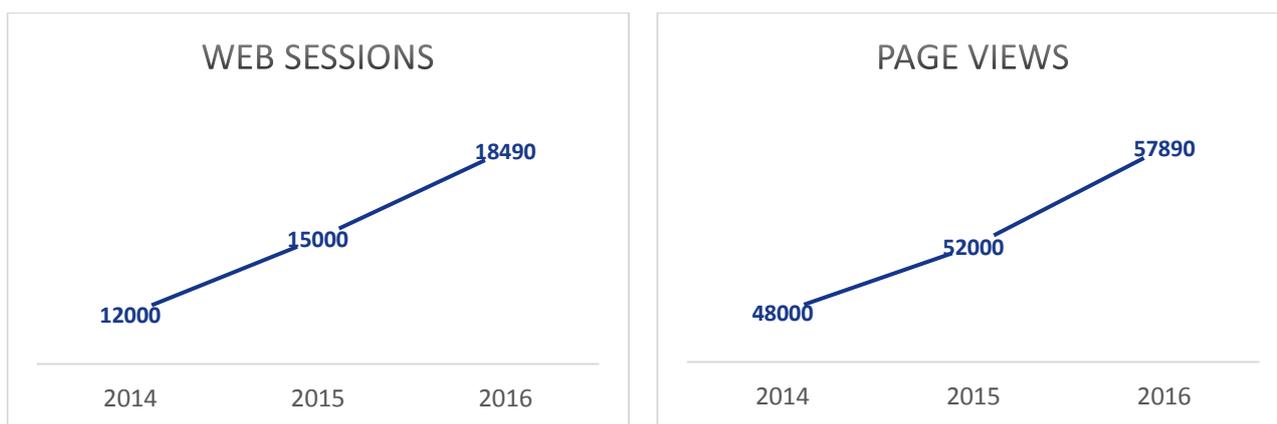


Figure 8: Overview of annual increase of ECSM web page sessions and page views.

### 5.2.2 NIS Quiz

The data in figure 9 indicates page views for the NIS Quiz reached 17,668 views out of a total of 57,890 views that the ECSM web site received in the period from 1<sup>st</sup> to 31<sup>st</sup> of October. These statistics show the popularity that the NIS quiz has gained during the campaign, equating to approx. 30% of the total ECSM site web traffic, almost 1/3 of the visits, targeted the NIS Quiz.



Figure 9: NIS quiz page views within ECSM October's events.

In more details, the results of the analysis have shown that:

- 7,514 page views were dedicated to accessing the main NIS Quiz page
- 2,051 page views were dedicated for accessing the introductory youtube video of the quiz

Nevertheless, in contrast to the encouraging numbers received above, it seems that only 788 visits resulted in the completion of the NIS quiz, which is 10% of the total amount of 7,514 visits to the quiz page, a rather sobering number.

### 5.2.3 ECSM Map of Activities

The following data from Figure 10 illustrate the number of activities taking place from 2013 to 2016 during October. The graph presents the total number of events registered on ECSM website during the month October every year since 2013.

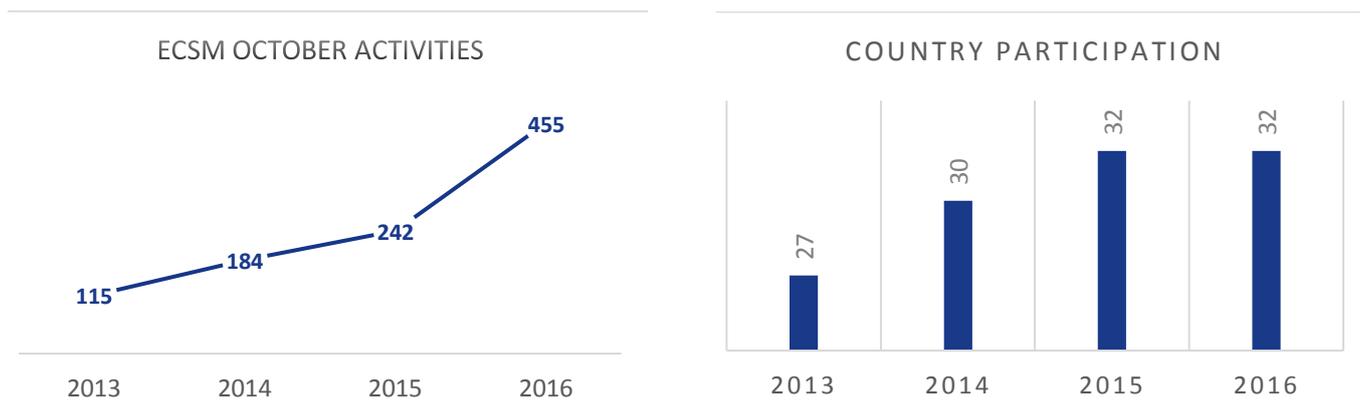


Figure 10: Number of activities in October and the number of countries registering activities on annual basis.

Clearly, a stable growth of events year on year occurred from inception up to 2015, wherein the number of events registered almost doubled in 2016 from the previous year.

The analysis has not taken into consideration the content of the events registered but only quantitative figures. The growth in the number of events registered is an outcome of the increased popularity of the campaign.

The second image in Figure 10 above represents the number of states in Europe that participated by registering events, while Figure 11 below illustrates the top ten countries with respect to the number of events they have registered during ECSM October month of events for 2016.

### TOP TEN 2016

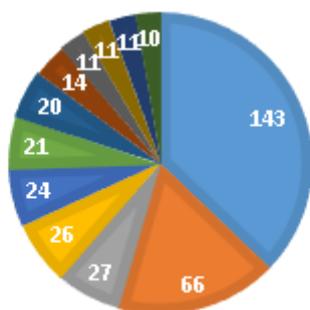


Figure 11: Top Ten countries with respect to the number of events registered.

More information on the content of such activities can be found directly upon accessing the official ECSM website.

#### 5.2.4 Social Media

Twitter has been a major tool used by ENISA to promote the campaign in recent years. Figure 12 below demonstrates the fluctuation of twitter followers from September until November 2016 for the handle @CyberSecMonth. The highest peak corresponds to the launch of ECSM and specifically the Kick-off event on the 30<sup>th</sup> of September, followed by renewed interest again at the later end of the month that coincided with Mobile Malware week.

Useful statistic that are extracted from the graph are:

- The total number of followers (6,847)
- The amount of new accounts (1,748) created within this period of three months

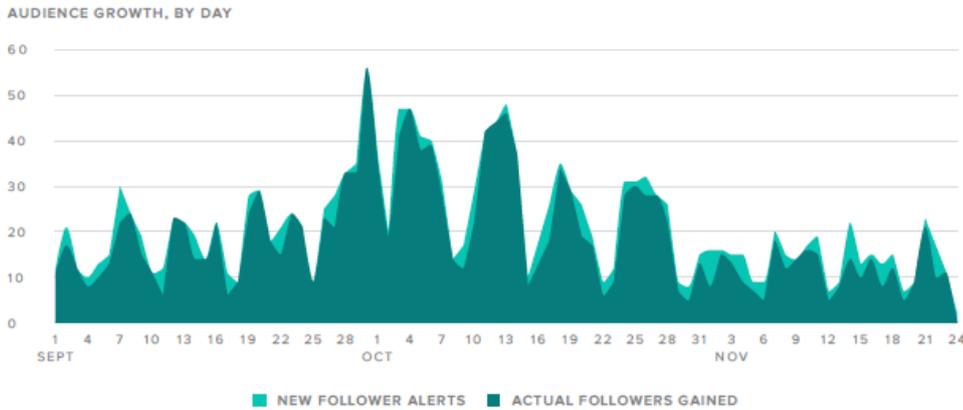


Figure 12: The daily growth of Twitter followers from September to November 2016 to @CyberSecMonth.

The graph below tracks the growth in the number of twitter followers to @CyberSecMonth over time. The graph illustrated in Figure 13 shows an accelerated growth in this year’s campaign versus the year on year growth from previous years.

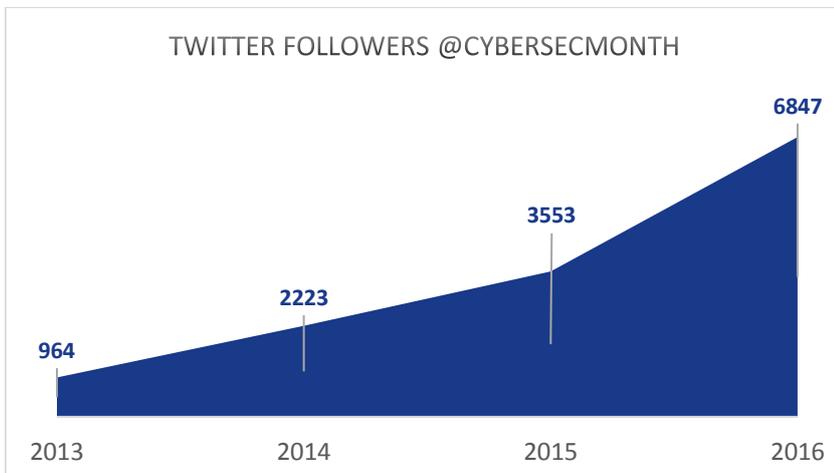


Figure 13: Annual number of Twitter followers @CyberSecMonth.

### 5.2.5 Media Reach

There were a total of 429 articles published which mentioned ECSM during October, including the 30<sup>th</sup> September of the kick-off event. In the charts below the reader can distinguish two major peaks. The first appears at the campaign’s kick-off date and the second peak occurs during the launch of the mobile malware week coordinated by Europol EC3.

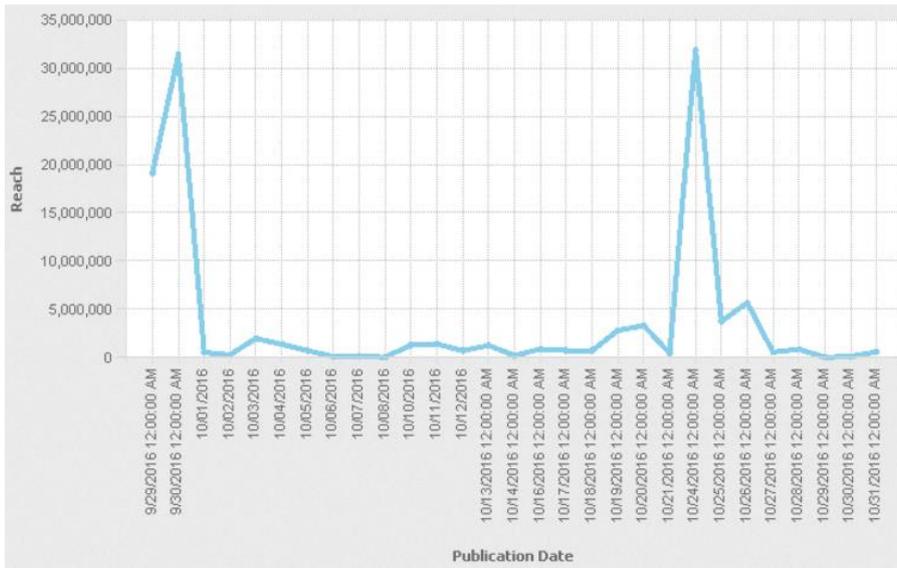


Figure 14: Estimated online reach in October 2016.

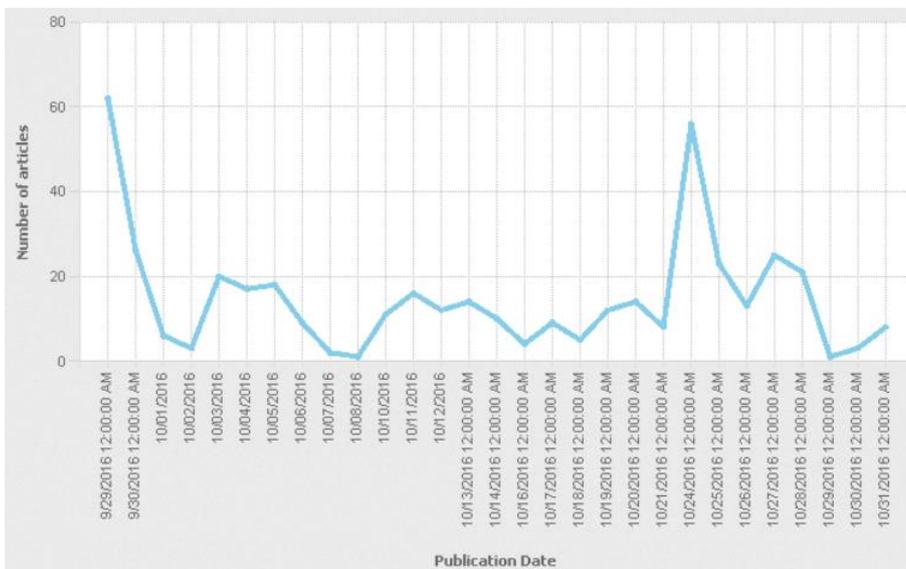


Figure 15: Number of articles published in October 2016 that mention ECSM.

The significant growth in the number of publications and online reach occurred in 2016 when compared to previous years, as demonstrated in the graphs below. Publications almost tripled year on year, while online reach, meaning the size of audience exposed to the campaign’s advertisement, almost doubled in size.

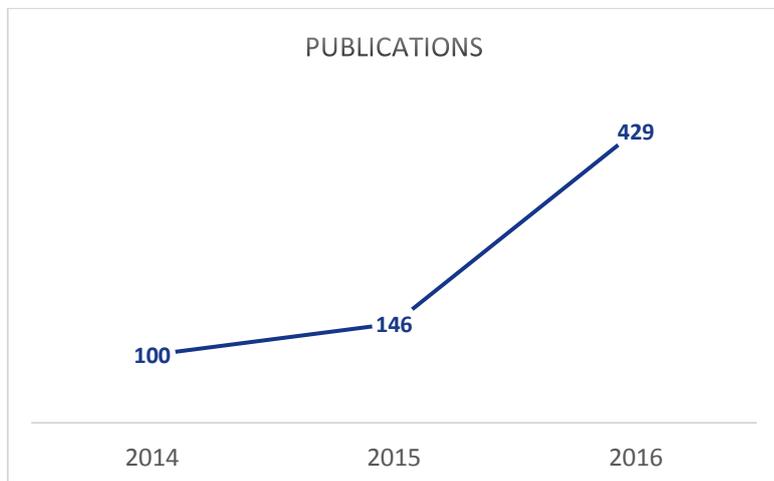


Figure 16: Overview of number of articles published during October overtime.

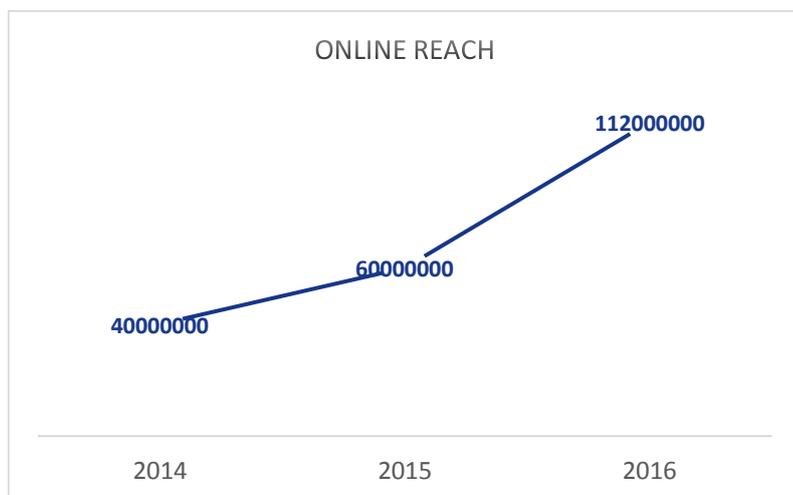


Figure 17: Online reach during October overtime.

### 5.2.6 Conclusions

The analytical indicators used to evaluate the campaign demonstrate a significant increase in growth year on year compared to the average level of growth from the previous years. What is significant is that this was a trend that span across a majority of the data points gathered for the evaluation, giving weight to the conclusion that the 2016 campaign outperformed that of previous years.

## 6. Conclusions and Future Work

---

The positive results of the evaluation coupled with the feedback received from the ECSM partners do not only confirm that the campaign was a success but they demonstrate that the campaign outperformed the results of previous years. Several factors contributed to this positive outcome, a major one being the strength of the relationship between ENISA and the national partners, another being the agreement with the European Banking Federation to host the kick-off event and another being the contribution of Europol's EC3 in the Mobile Malware theme of the week. Internally the readjustment in the working methods of the campaign also played a significant role in capitalizing on each of these factors.

A number of novel ideas also contributed to the campaigns success, such as the "Ask Me Anything" session on Reddit with F-Secure which reached the home page of Reddit with over 13 million subscribers, and the additional involvement of ECSM partners during the planning phase contributed positively to the campaign.

Taking a critical look at the campaign, the 2016 edition helped lay bare the strengths / weaknesses of the campaign, and raised questions on its vision and current trajectory. The reason for this revelation were two fold, a new coordination team and a revisiting of the initial objectives of the campaign. A new team was charged with the execution of the 2016 campaign, with this brought new fresh ideas to the table and good standing practices were scrutinized with new eyes. The chief concern for the new team was to ensure the continuation of the campaign in a similar capacity as the previous years so as not to jeopardise the existing efforts by knee jerk reactions. The second element was to return back to the original text of the pilot project of 2012, the awareness raising material produced by ENISA in that regard and also the Cyber Security Communications Strategy that was the driver for the campaign in the first place. The work performed during the pilot project, the objectives outlined in the Cyber Security Strategy and the documented awareness raising methods demonstrated that a schism had occurred between the current campaigns direction and the intended campaign direction based on these foundational documents.

The combination of these elements assisted in drawing up the following conclusions regarding the campaign:

### Strengths:

- Keen involvement by majority of EU Member States
- Campaign recognized across the IT Security industry

### Weaknesses:

- Minimal requests received by ENISA from Member States for support with their national campaigns
- Difficulty in evaluating the main objectives of the campaign given the current available data gathering practices
- The ECSM website not being used as intended
- Minimal private sector involved in the campaign
- Commitment from the European Commission is lukewarm
- Not all Member States are engaged in the campaign

The following points provide are a more detailed look at the shortfalls of the campaign:

- There is not a detailed and comprehensive communication plan produced to assist partners and coordinators with awareness raising, organizing press releases and social media activity

- The ECSM website is being used as an events gathering portal rather than its intended goal of providing awareness raising information and material to citizens
- There is minimal impact analysis done for the management of financial resources
- The work plan of the campaign was overly focused on the methodology rather than the goals and objectives of the campaign

ENISA will seek to address each of these points over the coming year. Already ENISA has sought the assistance of an awareness raising expert to help assess and evaluate the campaign with its goals and objectives. These risks will be further addressed during the process of assessment so as to mitigate them during 2017.

The success of the campaign over the past years and specifically for those of 2016 are tantamount to the strength of the ENISA brand to carry the campaign. It is this marriage between ENISA and ECSM that has formed the foundation that drives the popularity of the campaign; especially within the IT security industry. The question is; does the campaign have the momentum to continue as a standalone project?

### 6.1.1 2017 and beyond

The first point of call for 2017 is to attempt to re-align the campaign with the initial vision of the campaign as reflected in the seed documents. To this end, ENISA has requested the assistance of a security awareness raising academic to assess the campaign and help bridge the gap.

The 2016 edition highlighted many of the weaknesses and shortfalls of the campaign and these will be addressed in the coming year as documented in the conclusions, however the campaign can also benefit in a number of areas by considering the following aspects in the coming years:

- Making better use of social media channels to increase visibility and contact with citizens
- Seeking closer relationships and engagement with ECSM partners
- Using alternative means of communication with partners such as monthly newsletter and call for actions
- Producing a comprehensive list analytical indicators for evaluating the campaign

It is ENISA's hope that the campaign will continue to deliver results above expectations in the coming years and that issues raised within this report are addressed in order to provide the EU citizen with the tools necessary to act accordingly when online.

## Annex A: Infographics by Country 2016



### 2016 CYBER SECURITY ACTIVITIES BY COUNTRY



## CZECH REPUBLIC



**MOTTO:**  
Cyber Security and Safety  
is a Shared Responsibility

**LEADING ACTIVITY:**  
Promoting Safer Internet  
in Education, collaboration  
between stakeholders



#### Country Activities Map

|   |   |  |
|---|---|--|
| <p><b>CYBER SECURITY ROUNDTABLE</b></p> <p>Workshop with informal press conference for professional participants &amp; media focused on Cyber Security in Banking, Cyber Safety, Mobile Malware, Cyber Security Trainings</p> <p><b>THEMATIC LANDSCAPE</b><br/>Communicating cyber security and safety to people, administration and stakeholders</p> <p><b>VENUE</b><br/>3. 10. 2016<br/>Evropský dům,<br/>Jungmannova<br/>745/24,<br/>110 00 Praha 1</p> <p><b>FIND OUT MORE</b><br/><a href="http://www.ecsm.cz">www.ecsm.cz</a></p> <p><b>1</b></p> | <p><b>ONLINE BEZPEČNOST PRAKTICKY</b></p> <p>Traditional conference organized by NCBI in the frame of the project Prague-safe online. This year focusing on the best practice in the field of cyber crime prevention</p> <p><b>THEMATIC LANDSCAPE</b><br/>Addressing teachers, public administration, professionals of cybercrime prevention, LEA officers, media</p> <p><b>VENUE</b><br/>8. 11. 2016<br/>Magistrát hl. m. Prahy, Mariánské nám. 2, Praha 1</p> <p><b>FIND OUT MORE</b><br/><a href="http://konference.ncbi.cz">http://konference.ncbi.cz</a></p> <p><b>2</b></p> | <p><b>CYBER SECURITY COMPETITION</b></p> <p>Students of 1,400 secondary schools in the Czech Republic will be invited to participate in the Cyber Security Competition aiming to increase their digital literacy</p> <p><b>THEMATIC LANDSCAPE</b><br/>220,000 students will be invited to answer the questionnaire created by professionals and covering different practical aspects of the cyber security</p> <p><b>VENUE</b><br/>Online competition</p> <p><b>FIND OUT MORE</b><br/><a href="http://www.cybersecurity.cz">www.cybersecurity.cz</a></p> <p><b>3</b></p> |
|---|---|--|

#### Activities Implemented

**112**

#### Achievements & Metrics

|   |  |   |
|---|--|---|
| <p><b>CYBER SECURITY IN MEDIA</b></p> <p><b>483.000</b><br/>People addressed via mass media</p> | <p><b>CYBER SECURITY COMPETITION</b></p> <p><b>220.000</b><br/>Students addressed to take part in the Cyber Security Competition for secondary schools</p> | <p><b>CYBER SECURITY TRAINING</b></p> <p><b>465</b><br/>Attendees of professional conferences and workshops organized during the ECSM</p> |
|---|--|---|

#### Public, Private, NGOs and Regulatory Bodies Stakeholders Involved

**37**

**E-TRAINING LINKS**  
[www.ecsm.cz](http://www.ecsm.cz)

#eskills

#eEducation

#enisa

JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

**CYBER SECURITY IS A SHARED RESPONSIBILITY!**



The EU cyber security agency



[www.enisa.europa.eu](http://www.enisa.europa.eu) | [f](#) [t](#) [b](#) [v](#) [p](#) [g](#) [+](#)  
For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





# 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

## FRANCE



**MOTTO:**  
Acting collectively to meet the security challenges of the digital world

**LEADING ACTIVITY:**  
Raising awareness on cybersecurity issues, developing digital trust and training...



|  |   |  |
|--|---|--|
| <h3>Security Tips</h3> <ol style="list-style-type: none"> <li>1 Always use a unique and strong password for each account</li> <li>2 Keep your security software and web browser current</li> <li>3 Be wary of any suspicious emails</li> <li>4 Don't forget to save your important data regularly</li> <li>5 Never share your banking details through online communications</li> </ol>   | <h3>Country Activities Map</h3> <div style="display: flex; justify-content: space-between;"> <div data-bbox="558 784 957 1108"> <h4>CYBERSECURITY AWARENESS EVENTS</h4> <p>French experts will meet with private users, companies and administrations so as to raise awareness about cyberattacks and to give useful tips to face such threats</p> <p><b>THEMATIC LANDSCAPE</b><br/>Experts advices on cybersecurity issues</p> <p><b>VENUE</b><br/>All over France in October</p> <p><b>FIND OUT MORE</b><br/><a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>   #Banssi_fr   #TousSecNum</p> </div> <div data-bbox="957 784 1396 1108"> <h4>CYBERSECURITY AWARENESS ONLINE COMMUNICATION CAMPAIGN</h4> <p>What is a good password? How to protect my personal data? French experts will provide useful and easy tips to feel secure online.</p> <p><b>THEMATIC LANDSCAPE</b><br/>Digital security is everybody's business!</p> <p><b>VENUE</b><br/>All over France in October</p> <p><b>FIND OUT MORE</b><br/><a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>   #Banssi_fr   #TousSecNum</p> </div> </div> |  |
| <h3>Activities Implemented</h3> <p><b>17</b></p> <hr/> <h3>Public, Private, NGOs and Regulatory Bodies Stakeholders Involved</h3> <p><b>13</b></p>   | <h3>Achievements &amp; Metrics</h3> <div style="display: flex; justify-content: space-between;"> <div data-bbox="558 1164 957 1534"> <h4>DIGITAL SECURITY STRATEGY</h4> <p><b>1</b> common goal for both the private and the public sector</p> <p><b>2015</b> presentation of France's national digital security strategy</p> <p><b>5</b> objectives to reinforce collectively digital security in France and in Europe</p> </div> <div data-bbox="957 1164 1396 1534"> <h4>RAISING SECURITY AWARENESS</h4> <p><b>5</b> main audiences to reach :Companies, administrations, private users, schools, research. Whether it concerns the professional or the personal use of the Internet, everybody should be aware of the risks</p> <h4>FEELING CONCERNED</h4> <p><b>0-99</b> years old : it is never too soon or too late to be wise online !</p> </div> </div>  |  |
| <h3>E-TRAINING LINKS</h3> <p><a href="http://www.ssi.gouv.fr/particulier/precautions-elementaires">www.ssi.gouv.fr/particulier/precautions-elementaires</a>   #Banssi_fr</p>   | <p>#eskills   #eEducation   #enisa   JOIN#CyberSecMonth</p>   |  |
| <p>The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.</p> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: right;"> <h2>CYBER SECURITY IS A SHARED RESPONSIBILITY!</h2> </div> </div> |   |  |



The EU cyber security agency [www.enisa.europa.eu](http://www.enisa.europa.eu) | [f](#) [t](#) [b](#) [v](#) [p](#) [g](#) [+](#)  
For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





# 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

## GERMANY



**MOTTO:**  
Ins Internet – mit Sicherheit!

**LEADING ACTIVITY:**  
Promoting Cybersecurity for Private Users and Small and Medium Enterprises



Federal Office for Information Security

### Security Tips

- 1 Use strong passwords.
- 2 Keep your systems updated.
- 3 Don't open emails, if sender and subject are not plausible.
- 4 Use encrypted connections when transferring private data.
- 5 Don't log in to private accounts when using public Wifi-hotspots.

### Country Activities Map

#### ONLINE-SURVEY FOR PRIVATE USERS

For the second time we ask private users during the first half of October how they protect themselves online and which experiences they made regarding cybercrime. The results will be presented at the end of the month. The survey is a cooperation of the federal office

**THEMATIC LANDSCAPE**  
Security awareness of private users and experiences with cybercrime.

**VENUE**  
Online

**FIND OUT MORE**  
[www.bsi.bund.de/ECSM-Umfrage](http://www.bsi.bund.de/ECSM-Umfrage)

#### AWARENESS VIDEOS

For each weekly topic we produce an animated video which focuses on one aspect, like encrypted connection, use of public wifi, the risk of botnets and email-security.

**THEMATIC LANDSCAPE**  
Awareness raising

**VENUE**  
Online

**FIND OUT MORE**  
[www.bsi.bund.de/ecsm](http://www.bsi.bund.de/ecsm)

### Activities Implemented

**75**

### Achievements & Metrics

#### ONLINE-SURVEY FOR PRIVATE USERS

**1.724**

1724 private users took part in an online survey on protection measurements and experiences regarding cybercrime.

#### WEBINAR ON BASIC PROTECTION

**130**

In cooperation klicksafe and BSI organised a webinar for teachers on basic protection for IT. More than 130 persons wanted to register, which was more than the highest possible number of participants.

### Public, Private, NGOs and Regulatory Bodies Stakeholders Involved

**50**

### E-TRAINING LINKS

[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)  
[www.facebook.com/bsi.fuer.buerger](http://www.facebook.com/bsi.fuer.buerger)

#eskills #eEducation #enisa JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

## CYBER SECURITY IS A SHARED RESPONSIBILITY!



The EU cyber security agency [www.enisa.europa.eu](http://www.enisa.europa.eu) | [f](#) [t](#) [g+](#) [v](#) [p](#) [in](#)  
For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





# 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

## GREECE



**MOTTO:**  
I am Cyber Security updated!

**LEADING ACTIVITY:**  
Promoting Safe Internet in Education, Collaboration between Agencies



|  |   |  |
|--|---|--|
| <h3>Security Tips</h3> <ol style="list-style-type: none"> <li>1 If you are online you are vulnerable</li> <li>2 Stay updated, stay protected</li> <li>3 Do not enter personal data into electronic forms</li> <li>4 Do not open links from unknown sources</li> <li>5 Type in the the url yourself</li> </ol>  | <h3>Country Activities Map</h3> <div style="display: flex; justify-content: space-between;"> <div data-bbox="587 786 869 1093"> <h4>UNIFC2 FINAL WORKSHOP</h4> <p>Final demonstration and dissemination workshop of the UNIFC2 platform, preventing and fighting against cyber crime</p> <p><b>THEMATIC LANDSCAPE</b><br/>Fighting Cybercrime</p> <p><b>VENUE</b><br/>Athens, Greece</p> <p><b>FIND OUT MORE</b><br/><a href="http://www.unifc2.eu">http://www.unifc2.eu</a></p> </div> <div data-bbox="997 786 1359 1093"> <h4>81<sup>ST</sup> THESSALONIKI INTERNATIONAL FAIR</h4> <p>Hellenic Police had a booth providing information for safe browsing, cybercrime and cybersecurity, to the participants</p> <p><b>THEMATIC LANDSCAPE</b><br/>Cyber security</p> <p><b>VENUE</b><br/>Thessaloniki, Greece</p> <p><b>FIND OUT MORE</b><br/><a href="https://www.facebook.com/events/107305768947469/">https://www.facebook.com/events/107305768947469/</a></p> </div> </div>   |  |
| <h3>Activities Implemented</h3> <p><b>65</b></p>   | <h3>Achievements &amp; Metrics</h3> <div style="display: flex; justify-content: space-between;"> <div data-bbox="587 1173 869 1518"> <h4>CYBERKID CAMPAIGN</h4> <p><b>523.739</b></p> <p>More than 523.789 web page hits, more than 41.434 people visited the website and more than 4.084 downloads of the Cyberkid mobile application. From the total number of users the 44,4% were new visitors, while more than 1.395 facebook users like the Cyberkid page.</p> </div> <div data-bbox="906 1173 1173 1518"> <h4>RAISING SECURITY AWARENESS</h4> <p><b>2000</b></p> <p>2000 students have attended the "5<sup>th</sup> Safe Internet Browsing". Moreover, 49 workshops have taken place around the country, 13 schools have visited Greek Cybercrime Division and 3 teleconferences took place with school students attending. Finally, Hellenic Police participated in the 81<sup>st</sup> Thessaloniki International Fair, providing an information stand.</p> </div> <div data-bbox="1209 1173 1359 1518"> <h4>CYBERALERT CAMPAIGN</h4> <p><b>4.291</b></p> <p>More than 4.291 users have visited the website, with more than 10.204 web page hits and 75,6% new visitors. More than 103 have downloaded Feelsafe application, 445 Facebook users liked the page and more than 3.533 followers on Twitter.</p> </div> </div> |  |
| <h3>Public, Private, NGOS and Regulatory Bodies Stakeholders Involved</h3> <p><b>26</b></p>  | <h3>E-TRAINING LINKS</h3> <p><a href="http://www.cyberkid.gov.gr">www.cyberkid.gov.gr</a>   <a href="https://twitter.com/cyberalertGR">@cyberalertGR</a><br/><a href="http://www.cyberalert.gr">www.cyberalert.gr</a>   <a href="http://www.cybercc.gr">www.cybercc.gr</a></p> <p>#skills #eEducation #enisa JOIN#CyberSecMonth</p>   |  |
| <p>The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.</p> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: right;"> <h2>CYBER SECURITY IS A SHARED RESPONSIBILITY!</h2> </div> </div> |   |  |



The EU cyber security agency [www.enisa.europa.eu](http://www.enisa.europa.eu) | [@enisa](https://twitter.com/enisa)  
For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth





# 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

## HUNGARY



**MOTTO:**  
Cyber Security is a Shared Responsibility

**LEADING ACTIVITY:**  
Cooperation between Agencies, raising awareness, facilitate the network and information security of governmental agencies



### Security Tips

- Do not connect to unknown, unsecure wireless network (for example: hotel wifi).
- Protect your personal data online, check your security and privacy settings
- Don't click on unfamiliar links or unexpected attachments.
- Keep your system updated, always install the official software update.
- Do not use your private device for business issues

### Country Activities Map

#### CYBERSEC2016.HU

This 2 day-conference will be the opening of the Hungarian cyber security campaign. The conference is organised by the Cyber coordinator for the public and private sector representatives. The aim is to facilitate the PPP cooperation and discuss the main trends and challenges in cyber.

**THEMATIC LANDSCAPE**  
regulation, implementation, technical questions, NIS Directive

**VENUE**  
43 Teréz körút, H-1067 Budapest Hungary

**FIND OUT MORE**  
<http://www.cert-hungary.hu/cybersec2016.hu>

#### IN GATEWAY OF SCIENCE - POSTER CONTEST AND EXHIBITION

For years the National University of Public Service organize the "In Gateway of Science" - Poster Contest and Exhibition, which aims to provide a publication surface for students who are interested in science. This year Poster Contest and Exhibition organize a subsection for cyber security issues.

**THEMATIC LANDSCAPE**  
academia, exhibition

**VENUE**  
5 Ménesi út, H-1118 Budapest Hungary

**FIND OUT MORE**  
<https://www.facebook.com/events/1610455912581230/>

### Activities Implemented

**22**

### Public, Private, NGOS and Regulatory Bodies Stakeholders Involved

**21**

### Achievements & Metrics

#### CYBER SECURITY QUIZ

**1171**

In 51 days 1171 people filled in the online quiz of the National Cyber Security Center. This quiz was made for the governmental organizations to evaluate the general cyber security knowledge of the administrative staff.

Generally we got the correct answers for the questions of our quiz in 76%.

#### TRAINING FOR ELECTRONIC INFORMATION SECURITY MANAGERS

**100**

In compliance with the Hungarian IT security regulation ( called: Ibtv.), the National University of Public Service (NKE) launched a vocational training programme in 2014 to train Electronic Information Security Managers. Students enrolled in the program begin the fourth year of their studies in 2016. Until now, more than 100 professionals enrolled in the programme.

#eskills #eEducation #enisa JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

## CYBER SECURITY IS A SHARED RESPONSIBILITY!



The EU cyber security agency

[www.enisa.europa.eu](http://www.enisa.europa.eu) |

For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





## 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

# LITHUANIA



**MOTTO:**  
Smart in Cyber Security

**LEADING ACTIVITY:**  
Promoting Safe Internet in Education, Collaboration between Agencies



### Security Tips

- 1 Be a part of a safer internet
- 2 Cyber crime is a real crime. Do not ignore!
- 3 You are not only a viewer. You are a witness. React!
- 4 Do not open an attachment, if you're not expecting one
- 5 Do not trust a stranger on the Internet; fraudsters' imagination is boundless

### Country Activities Map

#### CYBER SAFETY DAY

Raising Security Awareness

**THEMATIC LANDSCAPE**  
Safe internet browsing

**VENUE**  
13. 10. 2016  
Secondary Schools

#### ARE YOU INTERNET GURU?

6 brain battle events (contests) with ICT security questions for teams of young unemployed people (INEET) all over the country.

**THEMATIC LANDSCAPE**  
ICT, cyber security, computer software and hardware.

**VENUE**  
6 Job Youth Centres

**FIND OUT MORE**  
[www.ldb.lt/Informacija/Veikla/Naujienos/UserDisplayForm.aspx?ID=7346](http://www.ldb.lt/Informacija/Veikla/Naujienos/UserDisplayForm.aspx?ID=7346)

#### Activities Implemented

8

#### AWARENESS CAMPAIGN VIA SOCIAL MEDIA

The awareness raising campaign using social and online media platforms of Lithuanian Safer internet centre partners.

**THEMATIC LANDSCAPE**  
Online safety

**VENUE**  
Lithuania

**FIND OUT MORE**  
[www.facebook.com/langasiateiti/6](http://www.facebook.com/langasiateiti/6)

#### BUILDING CAPACITY OF LITHUANIAN CSIRTS

Seminar to encourage efficient collaboration and build capacity of independently operating CSIRTS in Lithuania

**THEMATIC LANDSCAPE**  
Cybersecurity, CSIRT services, Collaboration

**VENUE**  
12. 10. 2016  
Lietuva  
Lithuania

**FIND OUT MORE**  
[www.nrdcs.lt](http://www.nrdcs.lt)

#### Public, Private, NGOs and Regulatory Bodies Stakeholders Involved

3

#eskills    
 #eEducation    
 #enisa    
 JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

## CYBER SECURITY IS A SHARED RESPONSIBILITY!



The EU cyber security agency



[www.enisa.europa.eu](http://www.enisa.europa.eu) |   
For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)   
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





## 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

# NETHERLANDS



**MOTTO:**  
Everyone safe on internet

**LEADING ACTIVITY:**  
Alert Online, annual awareness campaign, to increase cyber security skills and to make the Netherlands digitally safer.



Platform voor de Informatiebescherming

### Security Tips

- Undertake safety measures against ransomware
- Don't connect to public password-free wifi
- Make back-ups regularly
- Think before you post
- Use smart and strong passwords (or a password vault)

### Country Activities Map

#### ALERT ONLINE WEEKS

National awareness advocacy campaign to ensure a greater digital safety, by emphasizing the need for cybersecurity skills

**THEMATIC LANDSCAPE**  
Cybersecurity is an issue in the Netherlands. Get into action!

**VENUE**  
3-14 October

**FIND OUT MORE**  
[www.alertonline.nl](http://www.alertonline.nl)

#### CODEWEEK

Codeweeek events throughout the country

**THEMATIC LANDSCAPE**  
Coding at home, at school and everywhere!

**VENUE**  
15-23 October

**FIND OUT MORE**  
<http://codeweek.eu>

### Activities Implemented

**40**

### Achievements & Metrics

#### ZORG ZEKER CAMPAIGN (Ensure HealthCare Campaign)

**100**  
over 100 hospitals joined

stimulates awareness and own empowerment when dealing with private, personal information in healthcare

#### GAME OF TOONS

**10**  
with 10 teams of ethical hackers, making an attempt to hack Toon - an EMS of Eneco - and give feedback on the results

#### QUANTUM COMPUTING

**3**  
In a series of 3 public sessions about Cyberskills, this last session of KPN give a sneak peek of possibilities and the effects of quantum computing

### Public, Private, NGOS and Regulatory Bodies Stakeholders Involved

**196**

### E-TRAINING LINKS

[www.alertonline.nl](http://www.alertonline.nl)  
Facebook and Twitter @Alertonline

#eskills #eEducation #enisa JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

## CYBER SECURITY IS A SHARED RESPONSIBILITY!



The EU cyber security agency



[www.enisa.europa.eu](http://www.enisa.europa.eu) | [f](#) [t](#) [in](#) [p](#) [y](#) [+](#) [g](#) [+](#)  
For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





# 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

## POLAND



**MOTTO:**  
Be CyberSmart!

**LEADING ACTIVITY:**  
Promoting Internet Security and Safety by Education, Training and Collaboration between stakeholders.



### Security Tips

- 1 Be a part of a safer internet.
- 2 You are not only a viewer. You are a witness. React!
- 3 ISP - Internet Safety Providers.
- 4 Cyber crime is a real crime. Do not ignore!

### Country Activities Map

#### SECURE CONFERENCE

SECURE Conference is the important event in the calendar of meetings dedicated to IT security issues. The conference is addressed to administrators, security team members and practitioners in this field.

**THEMATIC LANDSCAPE**  
Leading international experts, specialized workshops, the latest solutions in one place, effective international networking

**VENUE**  
25-26 October  
Warsaw, ul. 17 Stycznia 24

**FIND OUT MORE**  
[www.secure.edu.pl/en/site/index.html](http://www.secure.edu.pl/en/site/index.html)

#### CYBER SAFETY

Cyber safety activities will include meeting of Polish ISP representatives, series of publications "What to do if..." and e-learning materials dedicated for teachers and pupils as part of KURSOR 2.1 project.

**THEMATIC LANDSCAPE**  
Online kids protection, E-learning, Meeting of experts, Publications

**VENUE**  
1-31 October

**FIND OUT MORE**  
[www.bezpiecznymiesiac.pl](http://www.bezpiecznymiesiac.pl)

### Activities Implemented

**7**

### Achievements & Metrics

#### SECURE 2015 CONFERENCE

**400**  
More than 400 participants; nearly 70 seminars; 4 hands-on workshops

#### QUIZZES AND CONTESTS

**26.000**  
More than 26.000 internet users have participated in Kursor Contest, online quizzes and second HackMe! Challenge.

#### ECSM 2015

**30.000**  
Approximately 30.000 of users have found out about cybersecurity month during October.

### Public, Private, NGOS and Regulatory Bodies Stakeholders Involved

**13**

### E-TRAINING LINKS

<http://bezpiecznymiesiac.pl>

#eskills #eEducation #enisa JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

## CYBER SECURITY IS A SHARED RESPONSIBILITY!



The EU cyber security agency

[www.enisa.europa.eu](http://www.enisa.europa.eu) | [f](#) [t](#) [p](#) [v](#) [y](#) [t](#) [u](#) [b](#) [e](#)

For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





## 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

# ROMANIA



**MOTTO:**  
Always watch for warning signs online

**LEADING ACTIVITY:**  
Promoting safe online behavior through education. 200,000 professional antivirus licenses for Romanian students.



Avira

|   |  |  |
|---|--|--|
| <h3>Security Tips</h3> <ol style="list-style-type: none"> <li>1 Think before you click!</li> <li>2 Use complex passwords!</li> <li>3 Limit availability of personal info!</li> <li>4 Backup your data regularly!</li> <li>5 Always be skeptical online!</li> </ol>  | <h3>Country Activities Map</h3> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <h4>ANTIVIRUS PROFESSIONAL LICENSE GIVEAWAY</h4> <p>AVIRA antivirus professional license giveaway to Romanian students (estimated: 200,000). The licences will be spread to the students registered to Ministry of Education database via CERT-RO website.</p> <p><b>THEMATIC LANDSCAPE</b><br/>Free professional AVIRA antivirus license giveaway</p> <p><b>VENUE</b><br/>CERT-RO</p> <p><b>FIND OUT MORE</b><br/><a href="http://www.cert.ro">www.cert.ro</a></p> </div> <div style="width: 45%;"> <h4>MOBILE MALWARE AWARENESS CAMPAIGN</h4> <p>Awareness campaigns involving cooperation with law enforcement for the organization of pop-up info points in transit locations in order to give information on the spot on mobile malware threats.</p> <p><b>THEMATIC LANDSCAPE</b><br/>Public places/Schools</p> <p><b>VENUE</b><br/>Public places/Schools</p> <p><b>FIND OUT MORE</b><br/><a href="http://www.cert.ro">www.cert.ro</a></p> </div> </div> |  |
| <h3>Activities Implemented</h3> <p><b>17</b></p>  | <h3>Achievements &amp; Metrics</h3> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <h4>ANTIVIRUS LICENSE GIVEAWAY</h4> <p><b>200.000</b></p> <p>All students registered to the Romanian Ministry of Education will have the opportunity to download a FREE professional antivirus license key from AVIRA via CERT-RO website.</p> </div> <div style="width: 30%;"> <h4>ROMANIA CYBERSECURITY EVENTS</h4> <p><b>20</b></p> <p>CERT-RO &amp; their partners team up for the ECSM to deliver the best cybersecurity awareness &amp; training events in Romania: conferences, hands-on trainings, workshops, courses.</p> </div> <div style="width: 30%;"> <h4>MOBILE MALWARE AWARENESS</h4> <p>CERT-RO teams up with the Romanian Police in a project implemented by EUROPOL for an awareness campaign regarding the rising mobile malware threat.</p> </div> </div>  |  |
| <h3>Public, Private, NGOs and Regulatory Bodies Stakeholders Involved</h3> <p><b>20</b></p>   | <h3>E-TRAINING LINKS</h3> <p><a href="https://cert.ro/doc/ghid">https://cert.ro/doc/ghid</a><br/><a href="https://answers.avira.com">https://answers.avira.com</a></p> <p>#eskills #eEducation #enisa JOIN#CyberSecMonth</p>   |  |
| <p>The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.</p> <p style="text-align: right;"><b>CYBER SECURITY IS A SHARED RESPONSIBILITY!</b></p> |  |  |



The EU cyber security agency



[www.enisa.europa.eu](http://www.enisa.europa.eu) | [f](#) [t](#) [g+](#) [v](#) [p](#) [in](#)  
For more information [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH





# 2016 CYBER SECURITY ACTIVITIES BY COUNTRY

## SLOVENIA



**MOTTO:**  
Internet fraud – it can happen to anyone

**LEADING ACTIVITY:**  
Promoting Safe Internet behaviour and rising awareness



REPUBLIC OF SLOVENIA  
MINISTRY OF PUBLIC ADMINISTRATION

### Security Tips

- Do not open an attachment, if you're not expecting one.
- Do not trust a stranger on the Internet; fraudsters' imagination is boundless.
- Don't be fooled by incredible offers!
- Don't be a jackass, get informed and protect yourself!

### Country Activities Map

**BUY ONLINE? OF COURSE, BUT WITH CAUTION!**

**THEMATIC LANDSCAPE**  
Fraudulent sellers online

**VENUE**  
Tehnološki park 19, 1000 Ljubljana

**ONLINE CAMPAIGN**  
Educational comic videos about most common online threats, online quiz 'Are you a web detective?'

**THEMATIC LANDSCAPE**  
Social engineering

**VENUE**  
31<sup>st</sup> - 31<sup>st</sup> October  
[www.facebook.com/varninainternetu](http://www.facebook.com/varninainternetu)  
[www.youtube.com/user/VarniNaInternetu](http://www.youtube.com/user/VarniNaInternetu)

**FIND OUT MORE**  
[www.varninainternetu.si](http://www.varninainternetu.si)

### Activities Implemented

**8**

### Achievements & Metrics

**ONLINE CAMPAIGN**

**40.000**  
More than 40,000 visitors on national cyber-sec awareness portal.

**ONLINE CAMPAIGN**

**1.000**  
users completed Web detective online Quiz

**ONLINE CAMPAIGN**

**500.000**  
More than online 500,000 views of comic educational videos about social engineering scams

### Public, Private, NGOs and Regulatory Bodies Stakeholders Involved

**8**

### E-TRAINING LINKS

<https://vni.cert.si/omfr> | [www.facebook.com/varninainternetu](https://www.facebook.com/varninainternetu)

#eskills #eEducation #enisa JOIN#CyberSecMonth

The European Cyber Security Month (ECSM) is an EU advocacy campaign. It promotes cyber security among citizens and advocates for change in the perception of cyber-threats, by promoting data and information security, education, sharing of good practices and competitions. Supported by ENISA and EC DG CONNECT.

**CYBER SECURITY IS A SHARED RESPONSIBILITY!**



The EU cyber security agency [www.enisa.europa.eu](http://www.enisa.europa.eu) | [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.cybersecuritymonth.eu](http://www.cybersecuritymonth.eu) | #CyberSecMonth

IN PARTNERSHIP WITH



## Annex B: ECISM 2016 - Map of Partners Activities' Logos



## Annex C: Kick-Off Agenda

### ECSM Kick-Off Event Agenda

| TIME          | TOPIC                           | SPEAKERS   |
|---------------|---------------------------------|--|
| 09.00 – 09.30 | Registration                    |  |
| 09.30 – 09.35 | Welcome                         | Sébastien De Brouwer, Executive Director, EBF  |
| 09.35 – 10.00 | Welcome speeches                | Wim Mijs Chief Executive, EBF<br>Steve Purser, Head of Core Operations, ENISA<br>Olivier Burgersdijk, Integrated Data Management, Europol<br>Ken Ducatel, Director, DIGIT  |
| 10.00 – 10.10 | Break                           |  |
| 10.10 – 10.40 | National Campaign Co-ordinators | Moderator: Vangelis Stavropoulos, Project Coordinator, ENISA<br>France: Anne-Charlotte Brou, Agence nationale de la sécurité des systèmes d'information (ANSSI)<br>Germany: Hanna Heuer, Federal Office for Information Security (BSI)<br>Luxembourg: Daniele Bisdorff, Ministère de l'économie du Luxembourg<br>Netherlands: Marjolijn Durinck, Platform voor de Informatiesamenleving (ECP)<br>Norway: Peggy Heie, Norsk senter for informasjonssikring (NorsIS) |
| 10.40 – 11.10 | Security in Banking             | Moderator: Keith Gross, Chair EBF, Cyber Security WG<br>Wien De Geyter, Secretary General, Febelfin<br>Troëls Oerting, Group Chief Information Security Officer, Barclays<br>Koen Hermans, Public Prosecutor, Eurojust<br>Peter, Kerstens, Advisor for Financial Sector Cybersecurity, DG FISMA  |
| 11.10 – 11.40 | Mobile Malware                  | Moderator: Olivier Burgersdijk, Integrated Data Management, Europol<br>Michael Shaulov, Head of Go To Market, Mobile Security, Check Point Software Technologies<br>Senan Moloney, VP Cyber Threat Intelligence, Barclays<br>Tomislav Vazdar, Chief Security Officer & Head of Corporate Security, Erste & Steiermärkische bank<br>Daniel Lawrence, Detective Inspector, NPCC National Cyber Crime PROTECT Coordinator, CERT UK                                    |
| 11.40 – 12.10 | Cyber Awareness                 | Moderator: Jakub Boratynski, Head of Cybersecurity and Digital Privacy, DG CNECT<br>Dr. Veronica Donoso, Executive Director, INHOPE<br>Dr. Hans Martens, Insafe network coordinator, European Schoolnet<br>Erka Koivunen, Cyber Security Advisor, F-Secure Corporation<br>William O'Connell, Chief Business Security Officer, ADP  |



## 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 Vasilissis Sofias  
Marousi 151 24, Athens, Greece



TP-04-17-027-EN-N



PO Box 1309, 710 01 Heraklion, Greece  
Tel: +30 28 14 40 9710  
info@enisa.europa.eu  
[www.enisa.europa.eu](http://www.enisa.europa.eu)

ISBN: 978-92-9204-218-9  
DOI: 10.2824/984485

