EUROPEAN
CYBER
SECURITY
MONTH

ECSM 2018 Deployment Report

JANUARY 2019

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.

Contact

For contacting the authors please use ecsm@enisa.europa.eu
For media enquiries about this paper, please use 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

ISBN 978-92-9204-280-6 DOI 10.2824/0844

Table of Contents

1. Executive Summary

Last year's joint communication to the European Parliament and the Council for the building up of cybersecurity for the EU included a call to Member States (MS) to make cyber-awareness a priority in awareness campaigns. The communication from the European Commission went on to explicitly mention the Cybersecurity month (ECSM) and how it should be scaled up to achieve a greater reach as a common communication effort at EU and national level.

This sets the scene for the 2018 campaign, the first campaign post the announcement. Indeed the 2018 European Cyber Security Month saw a step up by the MS in their engagement in the campaign. The number of MS taking an active role increased, however more importantly the collaboration of the MS in the planning and execution phases ensured that the sixth campaign continued to outperform previous years as measured by year on year results.

Highlights of 2018 campaign results:

- Number of activities increased by 6.5% from 532 to 567
- Number of twitter followers increased by 28% from 12894 to 16500
- Online reach increased by 4.6% from 86.5m to 90.5m
- Number of publications mentioning ECSM increased by 400% from 330 to 1655

The 2018 campaign was supported the European Commission, Europol's Cyber Crime Centre (EC3), European Schoolnet, SaferInternet4EU campaign and cyber security organisations from the Member States.

Just as in previous years the concept for the European Cyber Security Month is to address disparity of cybersecurity practices across member States in two stages. The first stage is to support the Member States so that the awareness and behaviour of citizens in each Member State is raised to a mature level. This becomes the reference baseline across the whole of Europe and thereby the European Cyber Security Month aligns the risk levels across Europe. The second stage is to further lower this risk by raising the maturity of citizen's behaviour in unison; at the European level. ENISA and the European Commission can achieve the objectives of the European Cyber Security Month by driving the pan-European campaign so as to ensure all Member States are actively committed to the European Cyber Security Month and that industry is also involved at all levels of the campaign both at the local and European level.

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 milestones 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 years. This year being the first year that the evaluation metrics developed in 2017 could be assessed using the previous year's base data. Although the evaluation metrics provided some insights into the evolution of the campaign at the MS level year on year, comparable results will only be comprehensive and robust once all Member States are providing evaluation metrics year on year. The report concludes with a conclusion and re-visits the future work described in the 2017 report.

Finally the report is intended to provide a basis for discussion among the Member States, the European Commission and ENISA on how the ECSM can best be organised in the years to come. All Member States will need to face up to similar challenges, namely how to engage citizens and organizations so as to affect their information security behaviour.

2. Introduction

With some 95 % of incidents said to be enabled by "some type of human error – intentional or not", there is a strong human factor at play, making cybersecurity everyone's responsibility. This means personal, corporate and public administration behaviour must change to ensure everybody understands the threat, and is equipped with the tools and skills necessary to quickly detect and actively protect themselves against attacks. People need to develop cyber hygiene habits and businesses and organisations must adopt appropriate risk-based cybersecurity programmes and update them regularly to reflect the evolving risk landscape.

The European Cyber Security Month (ECSM) under the coordination of ENISA is one of the mechanisms by which cyber hygiene and awareness is promoted to the citizens of Europe.

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, including the private sector, academia, the European Commission (EC) and other EU bodies, join together in a common vision by organising activities with special focus on training, conferences, 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 the participating MS for the 2018 campaign and presents the evaluation and conclusions of the campaign. More importantly, it seeks to trigger a discussion among partners with respect to improvements that can be made in the future.

2.1 Scope and Objectives

The scope of this report includes all the activities within the European Cyber Security Month (ECSM) campaign and their impact in 2018.

The main objectives of the campaigns within ECSM 2018 were as follows:

- to generate general awareness about Network and Information Security;
- to educate and enhance awareness of information security and privacy;
- to promote safer use of the internet for all users and the practice of basic cyber hygiene;
- to stimulate awareness of cyberscams;
- to build a strong track record to raise awareness through the ECSM;
- to involve relevant stakeholders and increase the participation of EU Member States;
- to increase national media interest through the European and international dimension of the project;
- to enhance attention and interest with regard to information security through political and media coordination.

2.2 Evaluation Methodology

In 2017, ENISA developed an evaluation strategy to guide the Agency and MS with the gathering of data and information for the evaluation of the campaign. The same evaluation strategy was employed in 2018. The Member State coordinators were urged to consider and define the evaluation metrics during the planning stage of the campaign, so that the right data and information would be collected during the execution stage.

The evaluation strategy includes both quantitative and qualitative approaches from the following sources:

- collection of quantitative data from the MS campaign coordinators,
- feedback from the MS campaign coordinators via the end of year Q&A questionnaire, and
- the use of media monitoring services to gather analytical data.

An evaluation data collection form was developed by ENISA in collaboration with the Member State coordinators for the purpose of information gathering. The evaluation form aims at extracting pertinent information on the overall activities involved in the MS campaigns, their potential impact and includes participants' feedback. The evaluation form was distributed to the Member State Coordinators in the form of an online survey, using the respective European Union platform EUSurvey (https://ec.europa.eu/eusurvey/), and ENISA requested the Coordinators to complete it depending on their national campaign strategy and execution. Guidelines accompanied the data collection form, that highlight recommended metics for each type of activity.

The evaluation strategy also included a questionnaire, where the aim was to extract information on the overall impact of the campaign based on MS campaign coordinators feedback with respect to ENISA's supportive role. Some of the elements assessed involve the level of support and its usefulness to MS, the impact of promotion material used and marketing strategies followed and the role of ECSM for improving the the outreach of MS campaigns.

2.3 Target Audience

This report is intended for organisations, either public or private, which supported the ECSM or intend to do so in the future. The report is also of interest to IT security professionals and other target groups who attended events and conferences organised across Europe. Further, the report targets EU national policy makers who aim to improve the security awareness of citizens, professionals and generally IT end-users.

3. Planning Phase

3.1 The role of ENISA in ECSM 2018

3.1.1 Vision statement

ENISA supports the Member States with the design and implementation of their awareness raising campaigns and to promote collaboration among EU Member States, international organizations and industry.

3.1.2 Mission statement

ENISA's mission for ECSM is to collaborate with the EU Member States and international organizations by finding innovative and fun ways to raise EU citizens awareness of cybersecurity, be they by organizing events, conferences, online quizzes, transferring of best practices or the use social media to educate and inform the public. Our mission is to enhance the delivery and synchronize ECSM among the EU Member States and industry that will share a pan-European vision and values for cybersecurity.

3.1.3 The Objectives for ECSM 2018

A consensus on the goals of ENISA for ECSM was reached with the participating MS. The goals that were recognized by all MS for the Agency are as follows:

- To promote the underlying value that is the foundation of ECSM:
  "Cyber Security is a Shared Responsibility"
- To assist the Member States in implementing ECSM activities that satisfy certain criteria: have well-defined objectives, have well-specified target audience(s) per activity, have systematically defined cybersecurity subjects, have systematically chosen delivery channels and techniques and have well-defined effectiveness metrics
- To support the Member States in defining common areas of concern for cybersecurity that are shared and will be commonly promoted to EU citizens
- To support the Member States in delivering at least one cross-border awareness raising activity among at least three EU Member States
- To support the Member States with collaboration with the private sector

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

- coordinator of the organisation of ECSM;
- hub for all participating MS;
- collector of available material and generator of synergies between MS;
- subject-matter expert on how to organise information security campaigns;
- subject-matter expert on how to design the content and evaluation strategy for information security campaigns;
- facilitator of common messaging within the participating MS 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 (infographics).

The Agency coordinated the organisation of the ECSM campaign, by acting as a “hub” for all participating MS and providing suggestions, replying to enquiries and generating synergies between MS where possible. The Agency assisted the participating MS in defining evaluation methods and metrics during the planning phase, in order to ensure the alignment of campaign targets and evaluation approaches.

3.2 Coordination

3.2.1 Conference Calls and Meetings

ENISA maintained regular communication with the MS, in order to enhance collaboration and cooperation amongst the MS. The Agency scheduled monthly conference calls for the MS to share their plans, receive and provide feedback and to support in the common promotion of the pan-European campaign strategy.

The Agency prepared and distributed the meeting agenda before each conference call. Meeting minutes where drawn up by ENISA after every call, and included a list of action points. The participation rate was high, with an average of 12 to 15 participates per meeting.

A physical meeting was organized by ENISA and held in Brussels in February 2018. The meeting gave MS the opportunity to discuss concerns and opportunities for improvements and finalize key areas of the campaign, such as the themes of the month, the collaboration infrastructure and the organization and decide on activities for the month.

3.2.2 Communication and Collaboration Technological Infrastructure

The collaboration mechanisms used for communication with MS is crucial for planning and executing the campaign. ENISA provided three types of software tools for maintaining communication:

- file repository and file exchange tools,
- teleconference software and
- tools for the communication and collaboration between Member State coordinators and third parties (e.g., the private sector)

3.2.2.1 File repository and File Exchange Tools

ENISA has been utilizing Sharepoint for accessing and storing files. The file repository facilitated the work of the MS that was previously supported with the exchange of files via email. Some MS however cannot access SharePoint due to security constraints.

3.2.2.2 Teleconference Software

Monthly conference calls were executed during the year in order to maintain regular contact with the MS. The selection of the teleconference software was noted as an important decision, given that there were a number of network and application restrictions on the side of the MS. In particular, certain tools (i.e., business versions, consumer versions) could not be utilised because they were restricted on the premises or the equipment of the coordinators’ public agencies.

3.2.3 Themes of the Month

ENISA organized a workshop on Feb 2018 in Brussels and invited the Member State coordinators to participate. The MS coordinators discussed and agreed upon the benefits of designing the MS campaigns around commonly agreed security and privacy themes. ENISA suggested during the workshop potential security themes and the MS discussed and debated on the most relevant and current topics based on MS cybersecurity priorities and the state of the art challenges. Following this discussion process, the MS gradually narrowed down the alternatives and determined four themes for the month, one theme for each one of the weeks in October.

The four themes chosen:

- Week 1 – Theme 1: Practice basic cyber hygiene
- Week 2 – Theme 2: Expand your Digital Skills and Education
- Week 3 – Theme 3: Recognize Cyberscams
- Week 4 – Theme 4: Emerging Technologies and Privacy

3.2.4 Press Releases

ENISA, with the input of the European Commission, drafted a press release for the official launch of the campaign. The press release included an overview of the campaign and quotes from senior officials. The press releases are translated into all the official languages of the EU and distributed to the Member State coordinators to support their formal press release announcements.

3.2.5 Kick-Off Video

During the ECSM workshop in Brussels the decision was made to release a kick-off video rather than organize a physical kick-off event. The MS & EFTA countries that participated in the kick-off video were France, Finland, Germany, Luxembourg, Norway, Malta and Poland. The video also included a message from Mariya Gabriel EU Commissioner for Digital Economy and Society.

The process for developing the video was organized into stages.

- ENISA proposed a script
- MS commented on the script proposal and made necessary changes
- Conference call was arranged with participating MS to finalize script
- Guidelines were produced by ENISA to standardized the clips from the MS
- MS chose the interviewee and formatted the prose based on the agreed upon script
- Final clips including name, title and translation were sent to ENISA to compile
- The clips were compiled to produce a single coherent set of messages and call to action
- A teaser video was produced and released a few days before the official release of the kick-off video
- The release of the official kick-off video coincided with the launch of the campaign

3.3 Evaluation Strategy

3.3.1 Evaluation Objectives

The Agency aimed to ensure that all Member State coordinators would capture information during the execution of the awareness campaigns to enable the overall evaluation of ECSM and its impact. The objective of the evaluation was to assess the effectiveness of the awareness activities, the attractiveness of the activity, and its potential outreach and impact. The Agency urged the Member State Coordinators to determine the evaluation metrics they would be using at the planning stage to ensure that they collected the necessary data come the execution stage.

3.3.2 Evaluation Metrics

The Agency developed an evaluation strategy and a set of evaluation metrics for the Member State Coordinators to use. The evaluation metrics were incorporated into a template evaluation form, for each coordinator to complete upon finalisation of the execution stage. The evaluation metrics were segregated per activity type, given that different information is relevant depending on the type of awareness campaign.

3.4 Marketing Material

Both the Agency and the Member States were committed to raising awareness. A series of marketing channels and material were used to achieve this purpose, as presented below.

3.4.1 Visual identity

The Agency created some years ago a visual identity for European Cyber Security Month including a logo[1], 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.

3.4.2 Slogan

The slogan “Cyber security is a shared responsibility!” remained unchanged in 2018.

3.4.3 Press releases

The Agency coordinated this year’s Press Release[2] with the European Commission, to ensure maximum outreach and to stimulate attention to the featured activities and events. The Press Release was translated into all official languages of the European Union and was released on the 28th September. The services of a media company were procured to further disseminate the press release to national and region journalists and press across Europe.

3.4.4 Social media - banners

The Web and Social Media banners remained the same as in the previous years.

The banner was available in four formats to match different needs (i.e., 815x315, 1500x500, 1200x717, 1200x630).

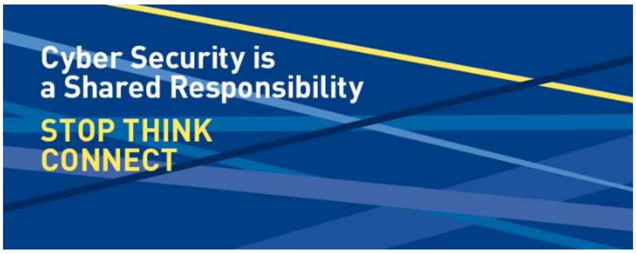


Figure 1: ECSM 2018 social media banner.

3.4.5 Poster and Infographics

During the physical meeting in Feb in Brussels the MS discussed the different marketing options and their impact. As a result of this discussion the MS decided not to produce posters for this year, but instead to allocate the relevant resources for the production of a kick-off video, because of its perceived higher impact and reach.

3.4.6 Kick-off video

A short kick-off video was produced with the support of a number of MS. The video included a general introduction to the campaign, core messages and a call to action.

3.4.7 Learning modules

Learning modules were created for each of the four topics for week two “Get Cyber Skilled”. For each of the four topics a guide was created with instructions and tips for the particular topics.

Topics:

[1] https://cybersecuritymonth.eu/press-campaign-toolbox/visual-identity

[2] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-shared-responsibility-2018-european-cyber-security-month-kicks-off

- Password management
- Backing up data
- Privacy settings
- Protecting against social engineering

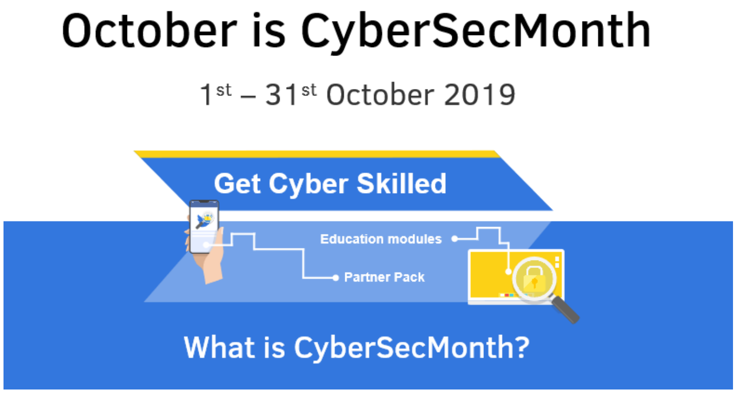
3.4.8 Toolkit for learning modules

A toolkit for week two was developed for the purpose of promoting the modules produced for week two campaign “Get Cyber Skilled”. This included a long and short copy, quotes from senior officials, core messages and cybersecurity tips.

3.4.9 Website

The material on the ECSM website[3] was re-organized including the tabs on the home page so as to enhance the accessibility of the website.

During week 2 for the theme Get Cyber Skilled the landing page was altered to promote the theme during the month as the graphic below demonstrates.



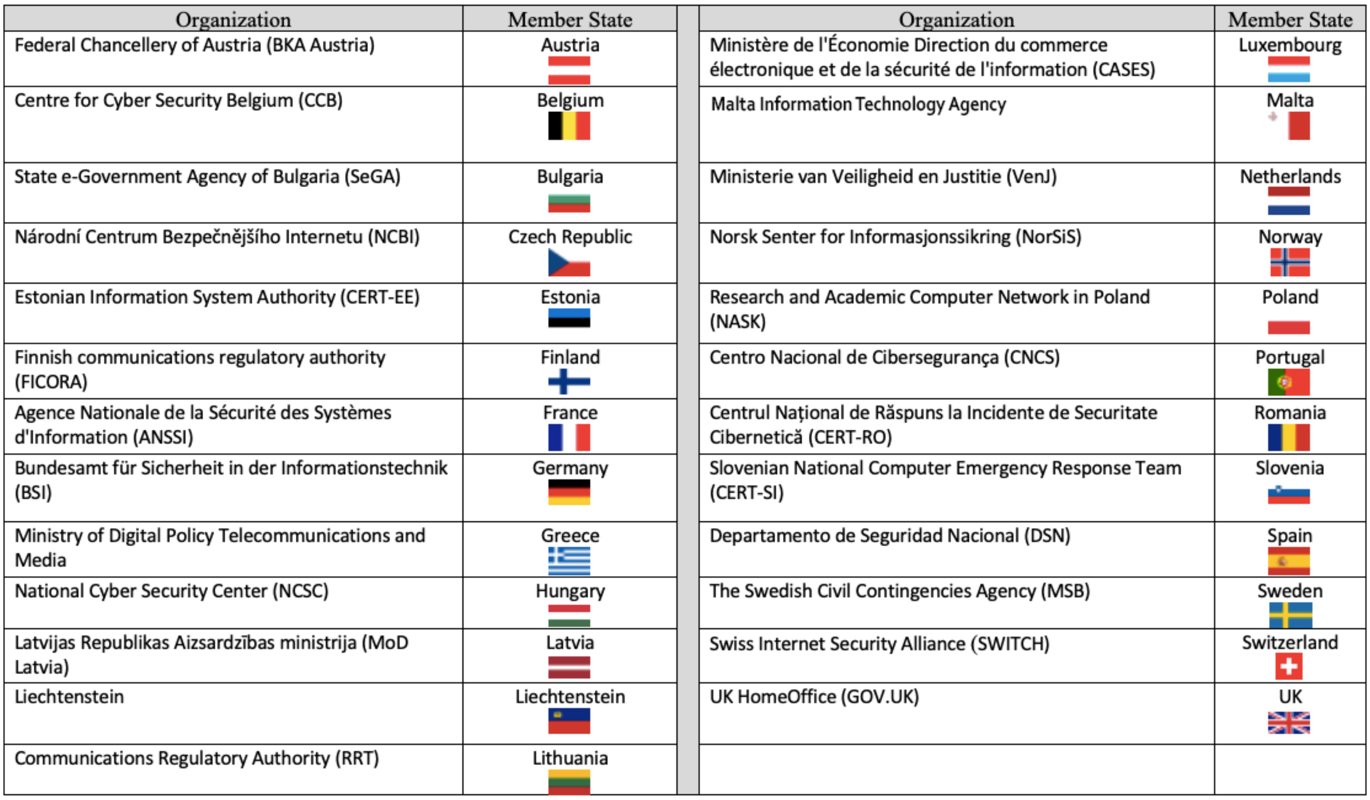
3.4.10 NIS Quiz

The NIS Quiz was not updated in 2018. It was decided at the ECSM meeting in February that the NIS Quiz would not be enhanced in favour for other activities.

3.5 MS Campaign Coordinators

The following table is a list of national campaign coordinators for ECSM 2018:

[3] https://cybersecuritymonth.eu/



Organization	Member State	Organization	Member State
Federal Chancellery of Austria (BKA Austria)	Austria	Ministère de l'Économie Direction du commerce électronique et de la sécurité de l'information (CASES)	Luxembourg
Centre for Cyber Security Belgium (CCB)	Belgium	Malta Information Technology Agency	Malta
State e-Government Agency of Bulgaria (SeGA)	Bulgaria	Ministerie van Veiligheid en Justitie (VenJ)	Netherlands
Národní Centrum Bezpečnějšího Internetu (NCBI)	Czech Republic	Norsk Senter for Informasjonssikring (NorSiS)	Norway
Estonian Information System Authority (CERT-EE)	Estonia	Research and Academic Computer Network in Poland (NASK)	Poland
Finnish communications regulatory authority (FICORA)	Finland	Centro Nacional de Cibersegurança (CNCS)	Portugal
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)	France	Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)	Romania
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany	Slovenian National Computer Emergency Response Team (CERT-SI)	Slovenia
Ministry of Digital Policy Telecommunications and Media	Greece	Departamento de Seguridad Nacional (DSN)	Spain
National Cyber Security Center (NCSC)	Hungary	The Swedish Civil Contingencies Agency (MSB)	Sweden
Latvijas Republikas Aizsardzības ministrija (MoD Latvia)	Latvia	Swiss Internet Security Alliance (SWITCH)	Switzerland
Liechtenstein	Liechtenstein	UK HomeOffice (GOV.UK)	UK
Communications Regulatory Authority (RRT)	Lithuania		

Table 1: List of ECSM campaign coordinators for 2018

4. Execution phase

4.1 Kick-off video

A teaser of the kick-off video[4] was released some days before the official launch of the campaign. This included clips from the commissioner and a call to action to take part in cybersecurity activities.

On Friday 28th September the ECSM video[5] was released with the official press release of the campaign.

The video included clips from the following:

- **European Commission** Mariya Gabriel|Commissioner Communications Networks, Content and Technology Informatics
- **Finland** Jarkko Saarimäki | Director of the National Cyber Security Centre at the Finnish Communications Regulatory Authority (FICORA)
- **France** Mounir Mahjoubi | Secretary of State for Digital Affairs
- **Germany** Arne Schönbohm | President of the German Federal Office for Information Security
- **Luxembourg** Francine Closener | Secretary of State of the Economy
- **Malta** Hon. Silvio Schembri | Secretary for Financial Services, Digital Economy and Innovation
- **Norway** Peggy Sandbekken Heie | CEO of Norwegian Centre for Information Security
- **Poland** Krzysztof Silicki | Director for Cybersecurity Capability Development and Cooperation

The event video has attracted over 1500 viewers since going live on the ENISA video channel on YouTube.

4.2 Themes of the month

Overview of the themes for 2018:

Week 1 – Theme 1: Practice basic cyber hygiene

ENISA and APWG designed a phishing poster for the first week of the campaign. The phishing poster provided information about the scale of the phishing problem by numbers, tips on how to avoid phishing and what to do if one becomes a victim of phishing.

Week 2 – Theme 2: Expand your Digital Skills and Education

The Get Cyber Skills campaign was launched on Monday 8th October. ECSM learning modules were created for the campaign with European Schoolnet (under a service contract with the EC for delivering the Better Internet for Kids core service platform and coordination of the Insafe network of Safer Internet Centres in Europe); and as part of the #SaferInternet4EU campaign launched on Safer Internet Day (SID) 2018 by Commissioner Mariya Gabriel to promote online safety, media literacy and cyber hygiene. This initiative stems from the Digital Education Action Plan and sets out a series of initiatives to support citizens, educational institutions and education systems to better adapt for life and work in an age of rapid digital change.

[4] https://www.youtube.com/watch?v=vWNUHaxensE&t=1s
[5] https://www.youtube.com/watch?v=ZlxR6nBYCLM&t=97s

Key message of the campaign –

Advancing cybersecurity skills and education of younger generations as an important means for keeping themselves and others safe. Just like the physical world there are threats online that could pose a danger to children and young adults physically, emotionally and financially. Building cybersecurity skills and competences helps the younger generation to develop routine cyber hygiene practices which they can then transfer to others and help protect society.

The target audience for Get Cyber Skilled campaign were parents, teachers, guardians, role models and community leaders responsible for developing cybersecurity education and skills in young people.

As part of the campaign, four ECSM learning modules were developed to help you create a study plan for your class. Topics include:

- Password management[6]
- Backing up data[7]
- Privacy settings[8]
- Protecting against social engineering[9]

The campaign included a toolkit[10] to help partners and Member States support with the outreach of the campaign.

Week 3 – Theme 3: Recognize Cyber Scams

The theme aimed at educating the general public on how to identify deceiving content in order to keep both themselves and their finances safe online.

The internet has become very attractive for cybercriminals. Attackers are using sophisticated tricks and promises to wrench money or valuable financial information out of users. Scams featuring a long-lost deceased relative or Nigerian princes are not the only tricks in the book anymore. The tactics used by cybercriminals are becoming increasingly innovative and harder to detect. From pretending to be the CEO of your organisation to impersonating a romantic interest, the online scammers of today will do what it takes to get what they want –money and/or banking credentials.

[6] https://cybersecuritymonth.eu/get-cyber-skilled/education-modules/education-modules/what-is-a-password-and-why-is-it-important

[7] https://cybersecuritymonth.eu/get-cyber-skilled/education-modules/education-modules/what-is-backup-and-why-is-it-important

[8] https://cybersecuritymonth.eu/get-cyber-skilled/education-modules/education-modules/what-is-social-enjineering-and-why-is-it-a-threat

[9] https://cybersecuritymonth.eu/get-cyber-skilled/education-modules/education-modules/what-is-social-enjineering-and-why-is-it-a-threat

[10] https://cybersecuritymonth.eu/get-cyber-skilled/partner-pack

As such, Europol and the European Banking Federation launched an awareness campaign on the 7 most common online financial scams.

Europol's European Cybercrime Centre (EC3), **the European Banking Federation** and their partners from the public and private sector participated in the campaign and included the **#CyberScams** awareness campaign as part of the European Cyber Security Month.

Law enforcement agencies from **all 28 EU Member States, 5 non- EU Member States, 24 national banking associations** and banks and many other cybercrime fighters raised awareness about this criminal phenomenon. This pan-European endeavour was driven by a communication campaign and national law enforcement, bank associations and financial institutions that was communicated via social media channels.

For this campaign, awareness-raising material was developed in 27 languages, available for public download, which includes information on the 7 most common online financial scams, and how to avoid them:

- **CEO fraud:** scammers pretend to be your CEO or senior representative in the organisation and trick you into paying a fake invoice or making an unauthorised transfer out of the business account.
- **Invoice fraud:** they pretend to be one of your clients/suppliers and trick you into paying future invoices into a different bank account.
- **Phishing/Smishing/Vishing:** they call you, send you a text message or an email to trick you into sharing your personal, financial or security information.
- **Spoofed bank website fraud:** they use bank phishing emails with a link to the spoofed website. Once you click on the link, various methods are used to collect your financial and personal information. The site will look like its legitimate counterpart, with small differences.
- **Romance scam:** they pretend to be interested in a romantic relationship. It commonly takes place on online dating websites, but scammers often use social media or email to make contact.
- **Personal data theft:** they harvest your personal information via social media channels.
- **Investment and online shopping scams:** they make you think you are on a smart investment… or present you with a great fake online offer.

Week 4 – Theme 4: Emerging Technologies and Privacy

Stay tech wise and safe with the latest emerging technologies.

The plan for week 4 of the campaign included a live webinar by ENISA experts and external experts from Industry with the purpose of discussing the importance of having an "Emerging Technologies Horizon Scanning and Research Process", however the activity was postponed to a later date.

4.3 Member State Campaigns Overview

The following section provides an overview of the campaigns executed at the Member State level, described in their own words.

4.3.1 Austria

A brief overview over some of the activities conducted in the course of the European Cyber Security Month (ECSM) in 2018 in Austria are presented below. While the timeframe of the ECSM itself is defined as 1st to 31st October, some of these activities did not take place within the month of October, e.g., because they are ongoing and/or take place over a longer period of time. Such activities are also valuable contributions to the ECSM and the overall goal of raising awareness for Cyber Security in Austria.

Austria IT Security Hub

Excellence can only be developed in a structured way through stable basic programs. The Austria Security Hub is a platform for an intensive and sustainable cooperation between a wide variety of companies and individuals in the cyber security environment and the education sector. At the same time, general IT security awareness is to be intensified at an early age and talents promoted through the ongoing activities of this platform.

Activity website: https://www.security-hub.at

Campus Lectures

The IT Security Competence Center of the FH Campus Vienna conducted a series of lectures called 'Campus Lectures' on a variety of Security topics, e.g. End-to-end Encryption (E2EE), the Austrian implementation of the GDPR (DSGVO) and its implications for those affected, IT Security Awareness in the times of IoT, Authentication on the Internet, the ZigBee standard often applied to so-called 'smart homes', the problem of (un)usability of many Security concepts experienced by users, Hacking World War II Electronic Bomb Fuses and CryptoCurrencies.

Activity website: https://www.fh-campuswien.ac.at

Information Security trainings for CISOs

The Association of Austrian Social Security Organisations has a CISO community which conducts regular Information Security trainings for CISOs of the respective organisations and together with the companies responsible for IT and chip card services. These are part of series of internal improvement measures in order to raise awareness for IT security.

Austrian Cybersecurity Challenge 2018

The Austria Cyber Security Challenge is the biggest security-talent (hacker) competition in Austria and reaches more than 500 participants as well as many schools and universities following this event.

Activity website: https://www.verbotengut.at/

Watchlist Internet - Information and warnings

The watchlist Internet provides To-date information and warnings regarding Internet fraud on their websites and social media channels.

Activity website: https://watchlist-internet.at

Saferinternet.at – Workshops, trainings, talks

A series of workshops for students, trainings for teachers and talks for parents drawing attention to cybercrime.

Activity website: https://watchlist-internet.at

Security Awareness @Gym-Kapfenberg

The FH Joanneum Kapfenberg conducted a Security Awareness Training for students.

IoT-Fachkongress 2018

This was a congress on Austrian Standards regarding Smart Cities and Country, Cloud and Security.

Activity website: http://bit.ly/iotecsm

ISC2 & ISACA: Security & Safety: 2 Denkschulen – 1 Ziel?

The Austrian Chapters of (ISC)2 and ISACA organised a series of presentations on Security and Safety and how those two concepts can be applied towards a common goal, which is the prevention of standstill, data loss and manipulation.

Activity website: http://bit.ly/iotecsm

Bits that Bite

The FH Burgenland organised an event with Keynote speeches about Meltdown Security Bug, data protection Basic Regulation, Firefox Privacy and IoT Applications.

Symposium Sicherheit

Erste Group Bak AG organizes every year a Security conference called the 'Symposium Sicherheit' for Security and Safety Officers in financial institutions. This was the 25th instalment of this series of conferences.

Activity website: https://www.erstegroup.com/symposium-sicherheit

IKT-Sicherheitskonferenz 2018

The Ministry of Defence organises an annual ICT Security Conference, which 2018 was held in Alpbach, Tyrol.

Activity website: https://seminar.bundesheer.at

Young Researchers' Day

SBA Research organizes jointly with the Austrian Computer Society the Young Researchers' Day. The Young Researchers' Day 2018 takes place in conjunction with the IKT Sicherheitskonferenz 2018 in Alpbach/Tirol (October 16 – 17, 2018), organized by the Ministry of Defence and Sports. The event takes place in line with the ACM SIGSAC Chapter Vienna and the working group IT-security of the Austrian Computer Society.

Activity website: https://seminar.bundesheer.at/pdfs/ProgYoung.pdf

Strategic Cyber Security Simulation Game

The Austrian Institute of Technology (AIT) conducted a strategic Cyber Security simulation, using a dynamic approach via an interactive questionnaire to simulate a threat scenario and corresponding decision-making.

Security Awareness Workshop with local security officers

The MD-OS/PIKT along with MA 01 (city of Vienna) conducted a Security awareness workshop for local security officers.

7th working session of the Austrian Cyber Security Platform

On 17.3.2015, the Cyber Security Platform (CSP) was set up with more than 100 stakeholders from business, science and administration. The CSP guarantees a periodic exchange of information on fundamental issues of cyber security, ensures the initiation of cooperation between the participating partners and forms an umbrella for already existing forms of cooperation (Austrian Trust Circle, Kuratorium Sicheres Österreich Cyber Sicherheit Forum, Centre for Secure Information Technology Austria, Cyber Security Austria, …). In addition, the platform of Cyber Security Platform Steering Group is available to provide assistance in an advisory capacity.

The platform aims to bring together existing activities and work groups without changing their structure and composition. The primary goal here is to make activities in the field of cyber security transparent for all stakeholders and to promote the formation of synergies. This platform aims not only to support the ongoing communication with all stakeholders but also intensify the collaboration between the public and private sector.

The 7th working session of the CSP was organised by the Federal Chancellery and held on 18 October in Alpbach, Tyrol.

Activity website: https://www.csp.gv.at

Security Potpourri 2018

The University of Applied Sciences Technikum Wien organised this regular event with speakers from the security industry and lectures on various topics in the area of Cyber Security.

Activity website: https://www.technikum-wien.at/security-potpourri/

Security Awareness @Kapfenberg

The FH Joanneum Kapfenberg organised a Security Awareness lecture for the local population of Kapfenberg.

IT Security Autumn

LSZ Consulting organised this event about latest IT Security Trends and Previews for 2019.

Activity website: https://www.lsz-consulting.at/events/it-security-herbst-trends-und-ausblicke-2019_255/

IT-SECX 2018

FH St. Pölten organised this conference about Secure Digitization.

Activity website: https://itsecx.fhstp.ac.at/

4.3.2 Bulgaria

We hereby briefly describe the activities carried out by CERT Bulgaria regarding the European Cyber Security Month 2018 (ECSM) campaign. The purpose of this year's ECSM campaign organized by CERT Bulgaria was to raise awareness among citizens and its constituency about how to protect their personal, financial and/or professional data.

We provide the details of our campaign's activities in a table format:

ACTIVITY	LINK	RESOURCES PROVIDED
First press release about the start of the ECSM 2018 campaign (28/09/18)	Website: https://govcert.bg/BG/NAW/Pages/Киберсигурността-е-споделена-отговорност---стартира-Европейският-месец-на-киберсигурността-2018.aspx	• Link to official European Cyber Security Month website: https://cybersecuritymonth.eu/ • Description of the main objectives of the campaign • Information about Cyber Security Month 2018 weekly topics • Link to ECSM kick-off video: https://www.youtube.com/watch?v=ZlxR6nBYCLM • Link to the ECSM activities interactive map: https://cybersecuritymonth.eu/activities/map • Links to the campaign in Twitter: @CyberSecMonth #CyberSecMonth, #OctoberNIS #CyberAware • Link to the ECSM 2018 quiz: https://cybersecuritymonth.eu/references/quiz-demonstration/intro
Announcement of the start of the ECSM 2018 campaign (4/10/18)	Twitter: @SeGovAgency https://twitter.com/SeGovAgency/status/1047844137142292480	• Links to the campaign on Twitter: @CyberSecMonth #CyberSecMonth, #OctoberNIS #CyberAware
Publication about one of the main threats – phishing (4/10/18)	Twitter: @SeGovAgency https://twitter.com/SeGovAgency/status/1047846620258349057	• Uploaded Phishing infographic in Bulgarian • Links to the campaign on Twitter: @CyberSecMonth #CyberSecMonth, #OctoberNIS #CyberAware
Publication about one of the main cyber threats – phishing (5/10/18)	Website: https://govcert.bg/BG/NAW/Pages/Фишингът---основна-заплаха-в-интернет-пространството.aspx	• Uploaded Phishing infographic in Bulgarian • Link to 2 video clips about phishing

		• Uploaded presentation about phishing threats and how to protect against them Link to 2 quizzes for phishing – for beginners and advanced
Cyber security awareness publication about passwords (10/10/18)	Website: https://govcert.bg/BG/NAW/Pages/Сигурността-на-паролите.aspx	• Link to a video clip about passwords • Link to a quiz for passwords • Link to ECSM 2018 learning modules: https://cybersecuritymonth.eu/get-cyber-skilled/education-modules
Publication for the ECSM 2018 campaign in CERT Bulgaria's digital monthly bulletin (11/10/18)	Digital monthly bulletin sent by e-mail to CERT Bulgaria's constituency, including publication about ECSM 2018 campaign	• Link to official European Cyber Security Month website: https://cybersecuritymonth.eu/ • Description of the main objectives of the campaign • Information about Cyber Security Month 2018 weekly topics • Link to ECSM kick-off video: https://www.youtube.com/watch?v=ZlxR6nBYCLM • Link to the ECSM activities interactive map: https://cybersecuritymonth.eu/activities/map • Links to the campaign in Twitter: @CyberSecMonth #CyberSecMonth, #OctoberNIS #CyberAware • Link to the ECSM 2018 quiz: https://cybersecuritymonth.eu/references/quiz-demonstration/intro
Cyber security awareness publication about passwords (11/10/18)	Twitter: @SeGovAgency https://twitter.com/SeGovAgency/status/1050305771878211584	• Links to the campaign on Twitter: @CyberSecMonth #CyberSecMonth, #OctoberNIS #CyberAware
Mobile security publication	Website: https://govcert.bg/BG/NAW/Pages/Защо-мобилната-сигурност-е-важна.aspx	• Link to a video clip about public networks security • Link to ECSM 2018 learning modules: https://cybersecuritymonth.eu/get-cyber-skilled/education-modules

Table 2: Overview of activities for ECSM in Bulgaria

4.3.3 Estonia

The CERT of the Estonian Information System Authority (RIA) decided this year to celebrate the October cyber security month by conducting small cyber-hygiene events all around Estonia. In addition to the employees of RIA we invited our partners from other government offices, schools and private companies (e.g., cyber security enterprises) to seek out potential local community audiences and talk to them about basic cyber hygiene.

This sort of action of mobilizing people around a communal project in their own communities has a long history in Estonia. Traditionally this has been an agricultural undertaking, for example the harvesting of potatoes. This is called “talgud” in Estonian. This year we decided to have “talgud” in the field of cyber security, where everyone who is able, could participate in their own communities.

The Cyber Security Month “talgud” event or roadshow started with an invitation. We invited schools, local libraries, general practitioners of medicine and other entities to sign up to these “talgud” – essentially inviting someone to come to talk about the importance of cyber hygiene. Then we assigned volunteer experts to the places. Altogether, about 30 people (half of them from RIA and half from our partner organizations) visited about 30 places on October 15th (with a couple of exceptions).

Among the offices where our experts went were:

- the staff of the Estonian parliament;
- two news organizations,
- schools and school-related organizations (school libraries, teacher assemblies, etc) and
- health centers.

Volunteer experts also called up their own childhood schools or health centers, where they visited the healthcare personnel and offered free trainings.

Among the volunteers were cyber security experts from RIA, experts from other government offices, employees and owners of private cyber security companies, diplomats and lawyers. In every part of the “talgud”, the volunteers were aided by leaflets and other materials provided by CERT-EE.

4.3.4 Finland

National Cyber Security Centre in Finland had two national online campaigns with social media activities during ECSM 2018. We also participated in the Cyber Security Nordic Conference and Exhibition with the Finnish Security Committee and Population Register Centre 10.- 11.10.2018.

We were active during #CyberScam-week also and took part in national cyber scam campaign with Finnish Police and Finance Finland (FFI) mainly in Twitter and Facebook.

We started ECSM month with our national password campaign "The longer the better". A password needs to be long enough, and it should not be too simple. We encouraged citizens to change their password to something safer.

Here's our *#thelongerthebetter* password video:

- https://www.youtube.com/watch?v=J7CVFv18ldw
- https://www.youtube.com/watch?v=JJq92PlHCC0 (Swedish version)

The videos were kind of overture to our main national campaign which started 8 November. The campaign ended during the first week of November.

The main character of Finland's national cyber security campaign was a middle aged man called “Teijo” who is very excited, and especially about passwords, backups and updates. He was very keen on giving advice about these themes to his colleagues at his workplace. Teijo also spread around cyber security themed aphorisms - #securisms - like "Life is short, password long" or "Hard work calls for hard updates".

We made three “1 minute” videos (in Finnish, with Finnish subtitles)

- Teijo and passwords
  https://www.youtube.com/watch?v=JXX9fm8P_20&list=PLcYs3a0AMHVl4VDNc56rybJtNFymTknUA&index=2
- Teijo and backups
  https://www.youtube.com/watch?v=rmhiPZ4j5sM&list=PLcYs3a0AMHVl4VDNc56rybJtNFymTknUA
- Teijo and updates
  https://www.youtube.com/watch?v=Mj_6XX6GpbM&

Humourous and carefully made video scripts with clear main messages were the keys to our campaigns’ success. Our strategy was not to try to say or teach everybody, everything at the same time. We support a “No more than 3 messages” approach. Hence, we focused on passwords, backups and updates.

4.3.5 France

The 6th edition of ECSM campaign was coordinated at the national level by ANSSI, the national authority for cybersecurity and cyberdefence, in France. The program of the campaign was ambitious, aiming to raise awareness and provide advice and recommendations in both the work place and at home.

For this year’s campaign, ANSSI, the national authority on cybersecurity and cyberdefence, worked alongside more than 20 institutional partners (ministries, association, non-profit organisation, national authorities, etc.) to build the national program all through October, focusing on the themes defined at the European level as well as the motto “Cybersecurity is a shared responsibility!’.

More than 80 activities were organized in France during the month. These activities involved:

- Conferences and workshops on cybersecurity issues for various events and audiences (companies, students, and administrations) hosted by the national ECSC partners such as ANSSI, the regional Chambers of Commerce and Industry, prefecture, etc.
- An active awareness campaign online, sharing tips and good practices all through the month with the #ECSM and #TousSecNum. The idea was to shed light onto the existing cybersecurity tool kit that includes infographics, videos, etc.
- Original activities :
  - First French participation to the European cybersecurity challenge (14th – 17th October) – a great event to promote cybersecurity skills and training (theme n°2)
  - The collaboration with a French cartoonist, Fix, to use humor and art as a way to raise awareness about cybersecurity. The cartoons were translated in English (subtitles). It also led to a common promotion of ANSSI (France) and BSI (Germany) productions on twitter.

MOI, ON ME LA FAIT PAS. JE SUIS QUELQU'UN DE PRUDENT : JE CHANGE RÉGULIÈREMENT LE MOT DE PASSE DE MON SMARTPHONE.
UN COUP, C'EST « 0000 ». L'AUTRE C'EST « 1234 ».
F:X
You know, I'm no rookie. I'm a careful man. I often update my pin code.
One time it's "1234", the other "0000"
MOIS EUROPÉEN DE LA CYBERSÉCURITÉ
BEN OUI, J'AI OUVERT LA PIÈCE JOINTE...
MAIS PAS LONGTEMPS !
F:X
du 1er au 31 octobre 2018
La sécurité du numérique est l'affaire et la responsabilité de tous !
#TousSecNum
Événement coordonné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec la participation des acteurs de la sécurité du numérique (associations, organisations professionnelles, autorités).
Pour en savoir plus : www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2018

Figure 2: Funny Cartoon Images used in the French Campaign to Promote Cyber Security Awareness

To promote ECSM messages and activities, a communication plan was defined by ANSSI and its partners including:

- Participation of the Secretary of States for digital Affairs, M. Mounir Mahjoubi to the kick-off European video
- Creation of a dedicated webpage on ANSSI's website to promote the ECSM activities : https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2018/
- Diffusion of a dedicated press release
- Regular publications on partners' website and social networks about ECSM, both in French and English (statistics to be consolidated)
- Creation of banners created for this 2018 edition to call people to take action and be part of ECSM on their social networks and website, using a communication kit.

4.3.6 Germany

The 6th edition of ECSM campaign was coordinated at the national level by BSI, the Federal Office for Information Security, in Germany.

General

In general, 192 events and local campaigns have taken place in Germany as part of the ECSM Cybersecmonth 2018. The BSI gained 104 partners, among them state ministries, criminal investigation departments, chambers of industry and commerce, associations, medias, enterprises and others. Moreover the BSI was focussing on Practice Basic Cyber Hygiene at home and at work.

Press

BSI published a press release[11] on the first of October. At the start of the ECSM a graphic visualising a "smart home" with four rooms was published on the website[12]. Each room contained one digital device.

Each week one room "opened" (as it turned from grey to coloured) and another digital device was the central theme for tips around IT-security at home. Within this topic the BSI presented facts and recommendations for more security around: router, computer, smartphone and IoT devices.

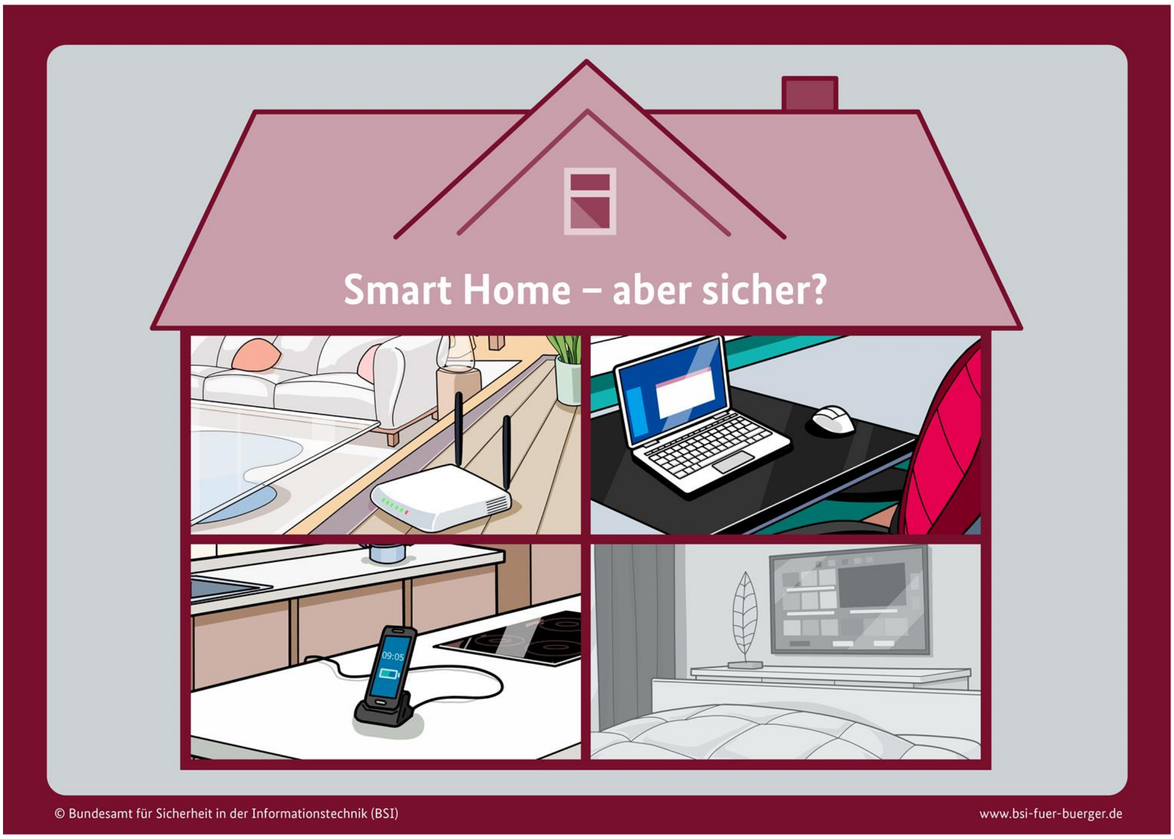

Smart Home – aber sicher?
09:05
© Bundesamt für Sicherheit in der Informationstechnik (BSI)
www.bsi-fuer-buerger.de

Figure 3: "Is your smart home secure?" - from the German ECSM Campaign

Social media

The BSI released four Facebook polls asking: "Be honest, how good is your cyber hygiene?"

- First week: Did you changed the password, when you first installed your router?
- Second week: Do you immediately install updates when available?
- Third week: Which kind of access authorisation do you permit your app?
- Fourth week: Do you know exactly what kind of data is stored by your wearable device?

Additionally the BSI published an awareness-video. Its central question is: Do you really have nothing to hide?' The advice and answer is: 'Take cyber security seriously to protect your privacy!'

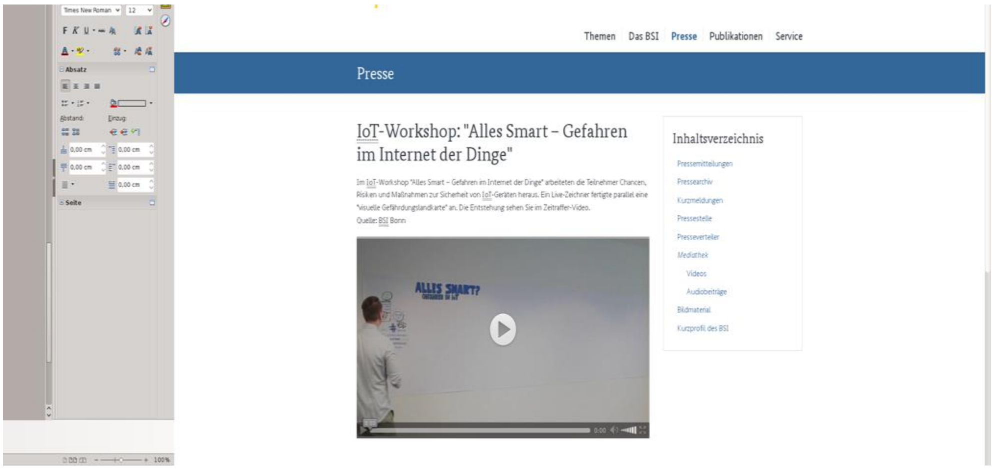
[11] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/ECSM-Start_01102018.html

[12] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/basisschutz_fuer_den_router.html

Furthermore the BSI intensified Social Media interactions with Europol, France, Belgie, Luxemburg and Sweden within Facebook and Twitter to show European ECSM actions in the BSI channels.

Events

The BSI organised a workshop to discuss opportunities and risks around the internet of things. During the event an illustrator painted an infographic containing all the ideas and input by the participants[13].



IoT-Workshop: "Alles Smart – Gefahren im Internet der Dinge"

Im IoT-Workshop "Alles Smart – Gefahren im Internet der Dinge" arbeiteten die Teilnehmer Chancen, Risiken und Maßnahmen zur Sicherheit von IoT-Geräten heraus. Ein Live-Zeichner fertigte parallel eine "visuelle Gefährdungslandkarte" an. Die Entstehung sehen Sie im Zeitraffer-Video.
Quelle: BSI Bonn

Figure 4: Risks and Opportunities along with IoT – from the German ECSM Campaign

Network

The BSI channel for economics distributed four illustrations[14] to raise awareness for cyber security among enterprises, organisations and institutions. The visuals were shared with the hashtag #ecsm by these partners and the BSI Twitter channels.

[13] https://www.bsi.bund.de/SharedDocs/Videos/DE/BSI/Interviews/IoT-workshop-bsi-2018-10-25
[14] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Awareness/awareness_node.html

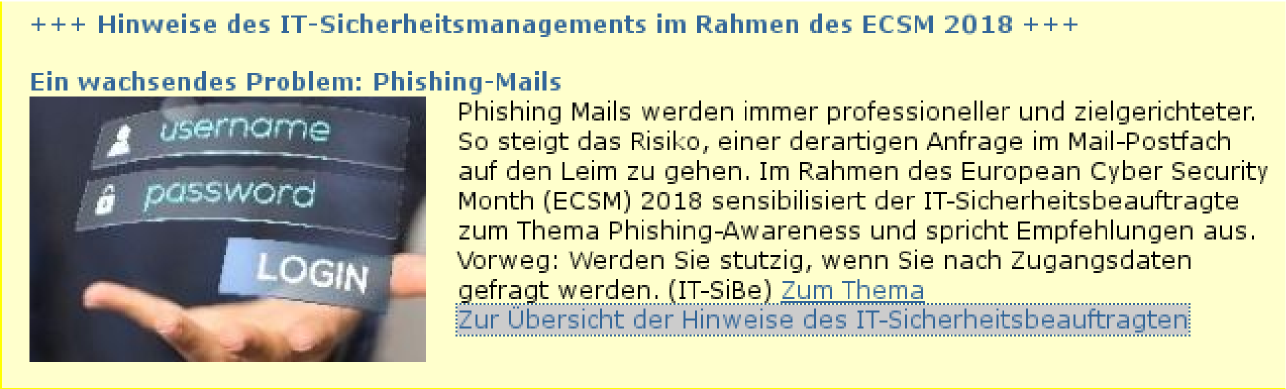
Schlüssel-Erlebnis
Mit gefälschten Benutzeroberflächen angeln Cyber-Kriminelle nach Zugangsdaten.
PASSWORD
Ins Internet – mit Sicherheit!
EUROPÄISCHER MONAT DER CYBER-SICHERHEIT
Allianz für Cyber-Sicherheit

© Bundesamt für Sicherheit in der Informationstechnik (BSI)

Figure 5: Key-Passwords in Cyber Security - from the German ECSM Campaign

Intern

Last but not least the BSI promoted the ECSM in the BSI-Intranet by informing employees about cyber risks day-by-day for one week. In the end employees were invited to take part in a quiz.



+++ Hinweise des IT-Sicherheitsmanagements im Rahmen des ECSM 2018 +++

Ein wachsendes Problem: Phishing-Mails

Phishing Mails werden immer professioneller und zielgerichteter. So steigt das Risiko, einer derartigen Anfrage im Mail-Postfach auf den Leim zu gehen. Im Rahmen des European Cyber Security Month (ECSM) 2018 sensibilisiert der IT-Sicherheitsbeauftragte zum Thema Phishing-Awareness und spricht Empfehlungen aus. Vorweg: Werden Sie stutzig, wenn Sie nach Zugangsdaten gefragt werden. (IT-SiBe) Zum Thema

Zur Übersicht der Hinweise des IT-Sicherheitsbeauftragten

Figure 6: About Phishing-Mails and Counter Protection - from the German ECSM Campaign

4.3.7 Hungary

In Hungary, ESCM2018 awareness campaign was coordinated by the National Cyber Security Center (NCSC Hungary).

The objective of the Hungarian campaign was to raise awareness for the Hungarian citizens (for several different groups and of different ages) about the main cybersecurity related topics, and to create better cooperation and professional discussions about the new cyber security trends and challenges.

As a campaign coordinator, NCSC-Hungary and its 25 campaign partners organised 34 different types of events or campaign elements (for example online campaign) between 28th September and 8th of November.

During the campaign there was a great variety of events in the programme: there were several conferences in different topics, awareness lessons at elementary schools, round table discussions, carrier discussions, cyber challenges for university students, cybersecurity “quiz shows”, cybersecurity escape rooms, university conferences, poster competitions and exhibitions, online campaigns etc.

To promote the ECSM campaign, the events, and the messages we used several communicational channels and awareness techniques:

- NCSC-Hungary created a website for the Hungarian ECSM campaign, where people can find info about the EU campaign, the Hungarian elements, events, posters and awareness materials, partners, photos about the evets and a cybersecurity online quiz also: https://kiberhonap.hu/
- NCSC- Hungary created a dedicated Facebook account for the ECSM in Hungary, where we posted the ECSM events, awareness materials, posters, videos and interesting articles about the ECSM topics: @Kiberhónap Magyarország
- NCSC-Hungary, Hungarian Police and the Hungarian Banking Association held a common press conference about phishing campaigns
- NCSC-Hungary organized a kickoff event, the Cybersec 2018.hu conference on 2th of October that has audience from the public and private sector and from the academia also.
- NCSC Hungary created a cybersecurity online quiz (2 level:1 for general users and for IT security experts)
- NCSC-Hungary created 2 Hungarian poster about the ECSM2018 campaign.

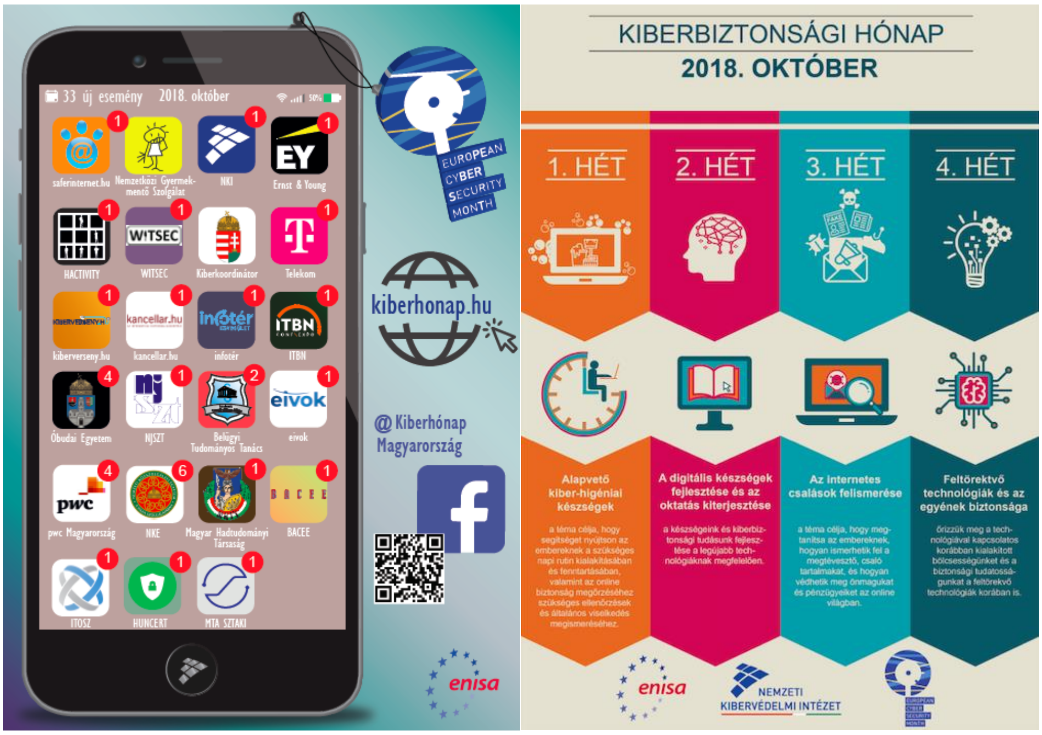

33 új esemény
2018. október
saferinternet.hu
Nemzetközi Gyermekmentő Szolgálat
NKI
Ernst & Young
HACTIVITY
WITSEC
Kiberkoordinátor
Telekom
kiberverseny.hu
kancellar.hu
infotér
ITBN
Óbudai Egyetem
NJSZT
Belügyi Tudományos Tanács
eivok
pwc Magyarország
NKE
Magyar Hadtudományi Társaság
BACEE
ITOSZ
HUNCERT
MTA SZTAKI
EUROPEAN CYBER SECURITY MONTH
kiberhonap.hu
@Kiberhónap Magyarország
enisa
KIBERBIZTONSÁGI HÓNAP
2018. OKTÓBER
1. HÉT
2. HÉT
3. HÉT
4. HÉT
Alapvető kiber-higéniai készségek
a téma célja, hogy segítséget nyújtson az embereknek a szükséges napi rutin kialakításában és fenntartásában, valamint az online biztonság megőrzéséhez szükséges ellenőrzések és általános viselkedés megismeréséhez.
A digitális készségek fejlesztése és az oktatás kiterjesztése
a készségeink és kiberbiztonsági tudásunk fejlesztése a legújabb technológiáknak megfelelően.
Az internetes csalások felismerése
a téma célja, hogy megtanítsa az embereknek, hogyan ismerhetik fel a megtévesztő, csaló tartalmakat, és hogyan védhetik meg önmagukat és pénzügyeiket az online világban.
Feltörektvő technológiák és az egyének biztonsága
őrizzük meg a technológiával kapcsolatos korábban kialakított bölcsességünket és a biztonsági tudatosságunkat a feltörekvő technológiák korában is.
enisa
NEMZETI KIBERVÉDELMI INTÉZET
EUROPEAN CYBER SECURITY MONTH

Figure 7: Posters on Cyber Security Awareness from the Hungarian ECSM Campaign

4.3.8 Luxembourg

In Luxembourg, the ECSM activities 2018 were carried out by 5 local partners, coordinated by the Ministry of the Economy. Partners this year were the Luxembourg Bankers' Association (ABBL); the national initiative for promoting a safer internet (BEE SECURE); the national Police; RESTENA CSIRT/UNI LU, and Security made in Lëtzebuerg - the national portal for promoting information security and the cybersecurity ecosystem.

EUROPEAN
CYBER
SECURITY
MONTH
EUROPEAN CYBER SECURITY MONTH
CYBERSECURITY IS A SHARED RESPONSABILITY
CYBERSÉCHERHEET BETREFFT ONS ALLEGUERTEN
LA CYBERSÉCURITÉ : UNE RESPONSABILITÉ PARTAGÉE
GEMEINSAM FÜR MEHR CYBER-SICHERHEIT
enisa
LUXEMBOURG
LET'S MAKE IT HAPPEN

Figure 8: Luxembourgish ECSM Campaign Banner

National activities included:

- social media posts
- a landing page for the Europol "cyber scams" campaign (see also here)
- Translation into Luxembourgish of the Europol information material
- a national awareness campaign on online relationships
- a cyber-day at University of Luxembourg campus,
- a dedicated Luxembourg cybersecurity week (15-20 October), with over 25 events including a Gala Awards evening

While all of the activities (gathering an estimated total of over 2000 participants) covered this year's ECSM topics, two of them specifically reached out to women in the cyber world. The Gala Awards evening (200 attendees) included a special address by Mariya Gabriel, EU Commissioner for Digital Economy and Society, and the presence of Mrs Despina Spanou, Director for Digital society, trust and cybersecurity at the EU Commission. Six awards were distributed: CISO of the Year; Best Inclusion Initiative; Most Promising Cybersecurity Solution (Jury's choice and people's choice); Best Talk; Most Promising Young Talent.

Thursday, October 18, 2018 at 17:30
CYBERSECURITY week
LUXEMBOURG
LET'S MAKE IT HAPPEN
Gala & Awards Night
CISO of the year // Most promising solutions // Best hack.lu paper
Best inclusion initiative // Most promising young talents

Figure 9: Cyber Security Awareness Event in Luxembourg – Gala e-Awards Night

“Be Cyber Aware”, an internal EC staff awareness raising initiative of the European Commission DG DIGIT, organised their “IT security day” in Luxembourg during the ECSM, with the possibility of a closer partnership in the future.

At national press level, 2 press releases were send out by the ministry of the Economy and articles were published in 6 local magazines/newspapers (*It nation; Paperjam; Silicon; Beast; Itone* and *Merkur).*

In view of the growing success of the “Luxembourg week” within the ECSM, we may consider extending the focus, from 1 to 2 weeks for the next edition.

All in all, the October month in Luxembourg contributed to increase the interest in cybersecurity with the public at large, raising visibility of public and private actors in charge, as well as to position Luxembourg as a key European player in cybersecurity.

4.3.9 Malta

During the European Cyber Security Month, Malta launched its second national awareness campaign for the coming years. This campaign intends to focus further on awareness and education in cyber security within various sectors of Maltese society. The Campaign was officially launched on Tuesday 16th October during an event held at Fort Sant’ Angelo, Birgu with keynote speakers being the Minister for Home Affairs and National Security, the Parliamentary Secretary for Financial Services, Digital Economy and Innovation, the ENISA Director, the Executive Chairman as well as the Head of Information Security and Governance of MITA – the Government IT Agency responsible for its implementation. Key stakeholders from the public and private sector were invited. The launch also led to the rollout of a new Website on Cyber Security as well as social media channels including Facebook, Instagram, Twitter and YouTube, apart from further use of traditional media such as radio, TV, newspapers and street advertising.

A ‘Capture the Flag’ Hackathon event – Malta Cyber Crusades 2018 was also held on 26th and 27th October, as a means to attract individuals towards cyber security skills uptake. It was open for individuals over 17 years of age. Over 40 persons, including students from tertiary institutions participated. This was the first of its kind held by MITA. Nonetheless a number of lessons learnt were taken note of for future considerations. They included further promotion prior to the event, further detailed training to beginners prior to the actual challenge, and prize categories for those already having expertise and those who are still beginners in such cyber security challenges.

Focus group sessions, in collaboration with Maltese SME representative bodies were also held on the 17th, 23rd and 26th October respectively. Such sessions served as a means to understand better the cyber security concerns and experiences amongst SMES and on ways of how related awareness can be reached to them more effectively. Amongst the lessons learnt were the need of other similar interactive or collaborative measures in the future as means for SMES to share knowledge and experience on cyber security, including awareness.

4.3.10 Norway

This year was the sixth time, The Norwegian Center for Information Security (NorSIS) has been the national coordinator for the National Security Month in Norway.

We have made a few changes this year, which we believe have been very successful. One of our changes is the broadening of our target group. Since our previous efforts and focusing on reaching small and medium sizes businesses, this time we have also been targeting the general population and larger businesses as well.

Although ENISA's campaign has four themes, we decided to concentrate on two themes, that is, "fake email" and "online fraud". This is on the basis of feedback from previous Norwegian campaigns.

Actions and activities

We kicked off the Norwegian Cyber Security Month with a free conference in Oslo the 27th of September. There were about 200 participants at the conference and about 100 people who followed the streaming of it on YouTube.

Our main effort and contribution to the campaign was the same this year as earlier years. The development, project managing and distribution of a security training kit for companies. This kit contains a presentation that managers are encouraged to hold for their employees in order to motivate them to follow an e-learning course on cyber security, also provided in the kit. The e-learning consists of 8 modules that take about 3-5 minutes to complete. Furthermore, the training package consists of films, brochures and other materials that managers can distribute in the office and among the employees to create awareness with regards to information and cyber security.

This year's e-learning reached 365 businesses with a total of 256,144 employees. This is a new record in reach which we are very pleased with. Part of this success may be because we have used a new e-learning provider this year. This has given us new opportunities for reaching larger businesses with the training kit. There is however a challenge with low figures for completion of the e-learning that we will need to address in next year's campaign.

In order to reach the Norwegian population with our messages about information and cyber security, we developed an e-learning course directed at the population. This course was launched on nettvett.no. The course intends to reveal attempts of social manipulation, ransomware, phishing and other types of fraud. Furthermore, it aims at helping the public to reveal fake contests and fake news in social media, teach them what to consider before sharing photos and videos online, securing their computers and mobile phones and detect fake emails.

In addition to the training kit, we facilitated a national lecture effort. Experts in information and cyber security donated their time and themed lectures as a contribution to the campaign. This is published on a website from which businesses can book lectures to educate and inspire their employees with people who daily work with information security at different kind of levels.

Creating awareness in social media has been a natural part of this year's campaign, for our core messages and advertising the training kit as well as supporting other efforts. One such initiative was the National Criminal Investigation Service (NCIS) with the spread of Europol's Cyberscam campaign in social Medias. The campaign was well made and a success in terms of sharing and reach in social media.

Finally, in addition to NorSIS's contribution, a number of experts, businesses, organisations and others have arranged, coordinated and participated at a number of conferences, meetings and seminars throughout the country in order to bring forward the message of "cybersecurity is a shared responsibility".

We look forward to continuing this work throughout the year of October 2019. We would like to take this opportunity to thank ENISA for your role and efforts in coordinating the European Cyber Security Month. We look forward to working with you on next year´s campaign.

4.3.11 Poland

European Cybersecurity Month in Poland is coordinated by NASK National Research Institute. The campaign has been organized for the sixth time but for the first time with such a flourish. A total of 45 initiatives has been reported and organized with cooperation of 30 partners and 7 honorary patrons: Prime Minister, Minister of Digitalization, National Security Bureau, Ministry of Science and Higher Education, Ministry of National Education, Ministry of Entrepreneurship and Technology, and Ministry of Health. The campaign started with the Kick-off event on 1st of October.

Inauguration was an open event which took place in "Przestrzeń from Facebook" with presence of 90 guests: partners, representatives of administration, academy, business, NGO's, media and citizens.

During the ECSM celebrations in Poland, a total of 45 cyber security initiatives and events took place. Some of them has been organized by NASK, some with cooperation with partners or partners alone. The main goal was to spread the information about ECSM campaign to the wide audience and this is why the initiatives were addressed to different target groups: professionals, children and adults, essential services providers, public administration and digital services providers. There were thematic conferences, experts meetings, workshops for children and youth, school activities, information campaigns and educational materials, open movies shows.

ECSM campaign was supported by communication held on the website www.bezpiecznymiesiac.pl - visited in October over 16,7 thousand times, which is a 75% of increase in comparison to previous year. For the first time ECSM in Poland was also present in social media. Thanks to the cooperation with Facebook, 1800 people socjety has been build on Facebook.

The campaign was also present on Twitter. Below are links to the ECSM social media:

- https://www.facebook.com/ECSMPL/

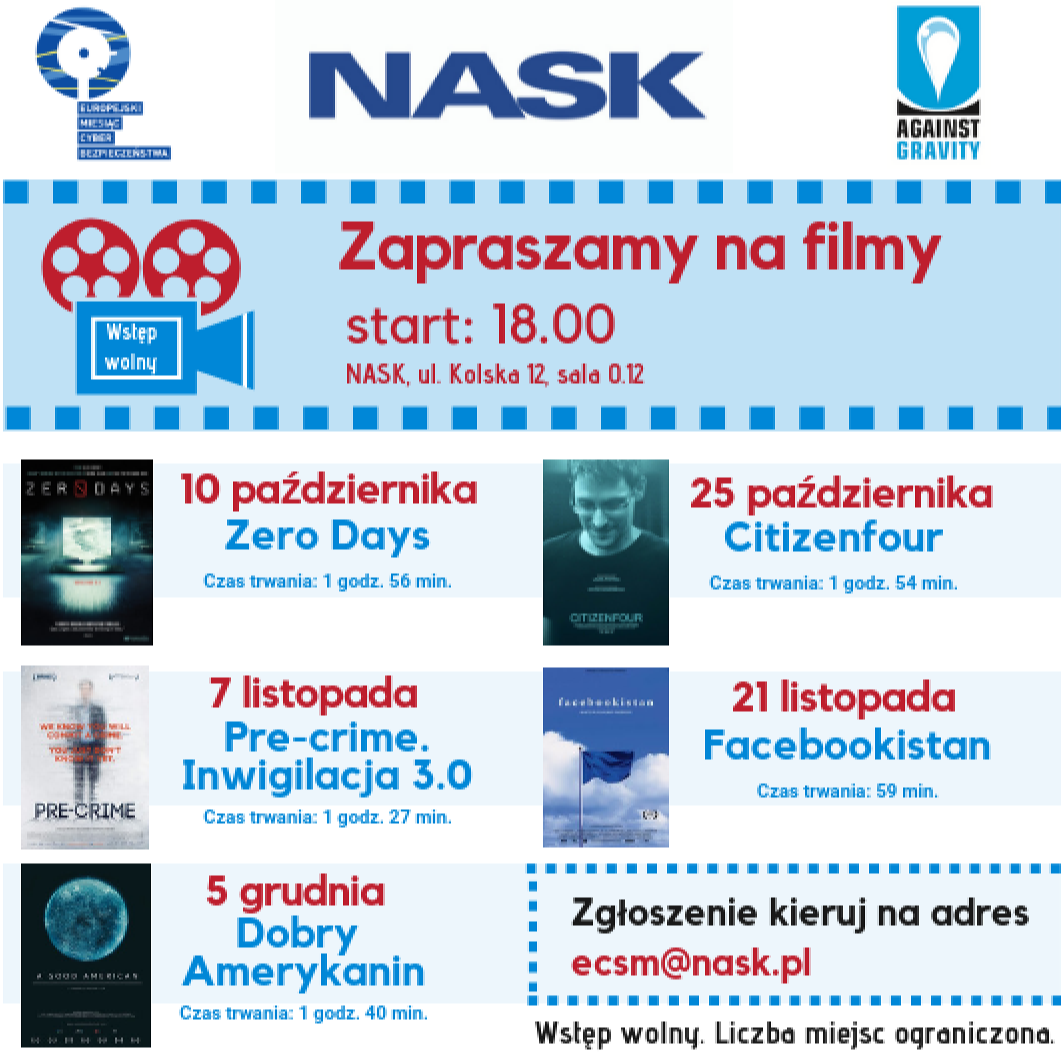
- https://twitter.com/EcsmPolska

The summary of all activities is presented on the NASK website and social media channel.

Some graphics produced for the campaign:

EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA
NASK
TYDZIEŃ I:
Cyberhigiena
Październik miesiącem cyberbezpieczeństwa

TYDZIEŃ III:
Scam
Październik miesiącem cyberbezpieczeństwa



EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

NASK

AGAINST GRAVITY

Wstęp wolny

Zapraszamy na filmy

start: 18.00

NASK, ul. Kolska 12, sala 0.12

10 października
Zero Days
Czas trwania: 1 godz. 56 min.

25 października
Citizenfour
Czas trwania: 1 godz. 54 min.

7 listopada
Pre-crime. Inwigilacja 3.0
Czas trwania: 1 godz. 27 min.

21 listopada
Facebookistan
Czas trwania: 59 min.

5 grudnia
Dobry Amerykanin
Czas trwania: 1 godz. 40 min.

Zgłoszenie kieruj na adres
ecsm@nask.pl

Wstęp wolny. Liczba miejsc ograniczona.

4.3.12 Portugal

The Portuguese National Cybersecurity Center (CNCS), the national point of contact with ENISA and in charge of raising awareness on cyber security, in 2018, similarly to previous years, carried out an awareness campaign within the scope of ECSM, which included offline activities - conferences, workshops, talks, awareness podcasts on radio programs and other initiatives - and online - cybersecurity tips, through the publication of posters, videos and posts on CNCS media channels.

In order to carry out this campaign, the CNCS had the involvement of national partners from different sectors - education, health, media, academia, industry, IT associations - without which it would be difficult to reach so many people.

The effort to convey the message that cybersecurity is a shared responsibility had positive outputs this year, leading to the increase of the number of CNCS partners to carry out these initiatives, as well as to the number of initiatives (in 2017 we have carried out 12 initiatives with 6 partners and in 2018 the number of initiatives increased to 40, 23 of them being organized by basic schools, and the number of partners increased to 40, being 23 of them schools). These activities were carried out in 30 cities or localities, distributed throughout the country, in addition to the awareness initiatives carried out online by CNCS and its partners.

It was found that the dissemination materials available on the ECSM website and the sharing of the materials and information about campaigns that were being carried out by other countries were very useful and served as inspiration for activities and initiatives in other countries or places.

4.3.13 Romania

This year's ECSM 2018 campaign in Romania, we focused more than ever on social media interaction with common users. Some of our main activities involved:

- Social media cybersecurity awareness campaign (Facebook, Twitter, LinkedIn, Instagram, YouTube).
- On CERT-RO and partners social media channels we scheduled 3 to 4 daily posts on ECSM 2018 main themes.
- Fostering new public-private partnerships, with organizations very much interested in cyber security awareness campaigns
- Partnership with Digital Nation for FREE one month vouchers for cyber security course (12 months) if users sign in during ECSM2018 campaign.
- Partnership during ECSM2018 with PentestTools.com for FREE 250 credits that could enable users to do multiple testing of their website security.
- Ask me Anything campaign with CERT-RO team in the last day of the campaign on Reddit (r/Romania)
- Like every year, we managed to have a cyber security course for influencers (journalists) during ECSM2018.
- Support for other campaigns during the month of October: CodeWeek, CodeKids, Safety in Online (highschool campaign).
- Support and direct involvement in the process of selection and training of Romania Team for European Cyber Security Championship 2018
- Cyber Security exercises: CyDex2018 (national cyber security exercise in Romania).
- The CERT-RO annual international conference on cyber security during the month of October. The event has always been part of the ECSM calendar of events in Romania.
- Support for Europol and EBF campaign against online fraud on all channels.
- TV news pieces regarding pressing cyber security issues and ongoing campaigns against RO common users in online: vishing, phishing, scam.

Some Issues that we identified with respect to the ECSM calendar for editing by CERT-RO. In this context, we found a great dependency on ENISA for any encountered issues, also in order to change info on events. A higher control over what is published over Romanian events is recommended in the future.

Some additional remarks include that we need more materials that are formulated with a clear message. We think that the materials provided by Europol are a great example in that direction. Also, we support more video/gif materials for users. People are less inclined to read and social media is much happier to push multimedia content on their channels. Organic reach could get much bigger this way.

4.3.14 Spain

In the light of the Cyber Security Month campaign, Spain organized a set of activities to promote awareness and culture in cybersecurity.

There were several Organisms involved: Guardia Civil, National Police, National Institute for Cybersecurity (INCIBE), National Cryptologic Centre (CCN), National Security Department, … Regarding the private sector, there were many events and actions focused on that.

All these Organisms and Companies spread information by using their communications channels (webs, social networks, etc.).

The most important event on October has been ENISE (12TH edition of the International Meeting on Information Security, organized by the National Institute for Cybersecurity -INCIBE-), the major conference on Information Security that gather top experts, investors and stakeholders in the sector, where more than 1.000 people attended.

The media content produced by Europol and financial sector, in collaboration with Law Enforcement Agencies, delivered during the 3rd week (focused on Cyber Scams) was useful, and this model (making resources in collaboration with European agencies), could be extended to the rest of activities.

Finally, is very welcome the initiative from ENISA for this year's ECSM, according to which a National Coordinator can approve, modify or deny the events before they are published at the ECSM website's portal.

5. Evaluation

5.1 Assessment of Implemented Actions based on the Evaluation Methodology

The evaluation metrics are a useful tool for collecting consistent information from MS coordinators regarding the activities that they implemented during the ECSM. Given the different nature of the variant ECSM activities, the evaluation methodology defined different metrics per type of activity. The following categories of activities were identified and accompanied by respective metrics:

- Conference/ Workshop activities
- TV or Radio Advertisement activities
- ECSM Website
- Social Media Activities
- Fair Stand/ Exhibition and Roadshows
- Merchandising, Posters, Leaflets
- Tests/Quizzes
- ECSM Organization Effort

The following Member States, provided data for 2018:

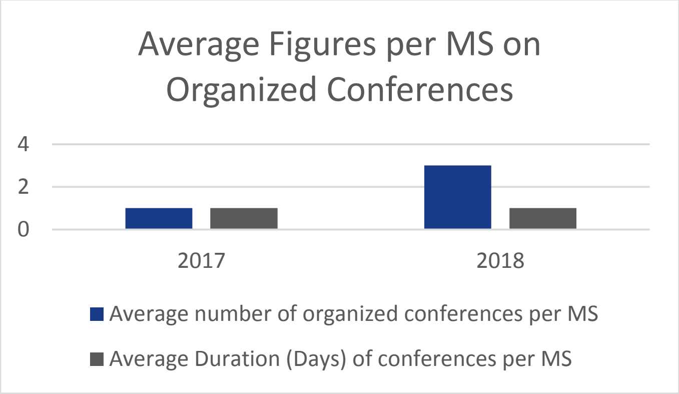
- Belgium
- Bulgaria
- Estonia
- Finland
- Germany
- Hungary
- Luxembourg
- Malta
- Poland
- Portugal
- Romania

The following Member States and EFTA countries, provided data for 2017, the base year of the evaluation:

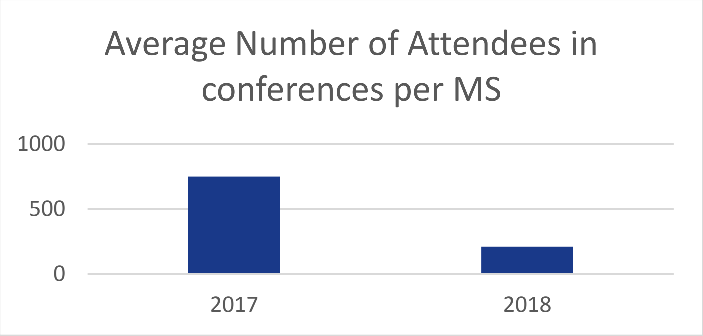
- Czech Republic
- Germany
- Latvia
- Luxembourg
- Norway
- Poland
- Slovenia

5.1.1 Results for Conference/ Workshop activities

The following figures demonstrate the average number of activities per MS with regards to the organization of conferences and workshops for 2017 and 2018.

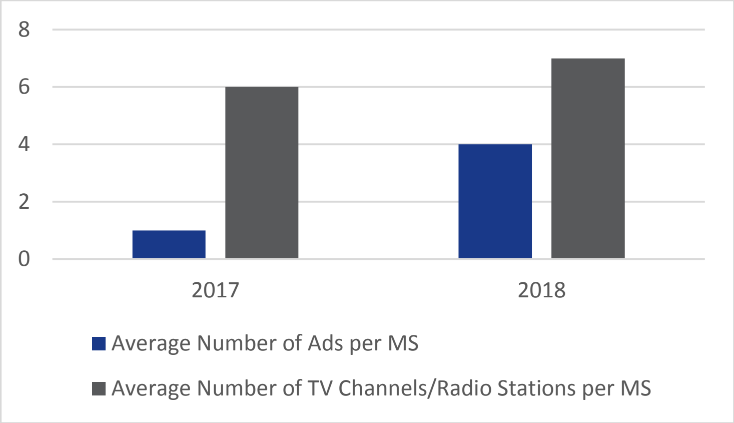


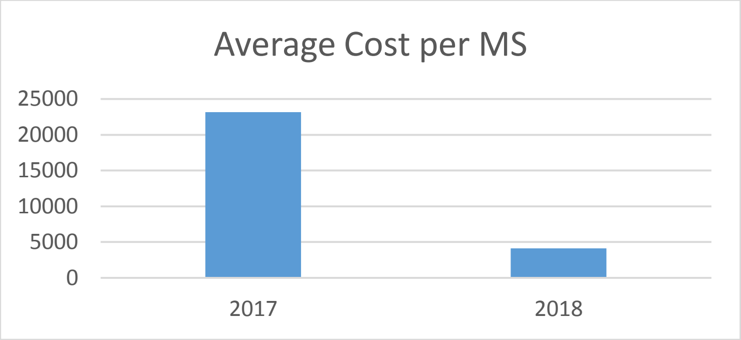
On average MS organized more events in 2018 compared to 2017, however the duration of the events were maintained year on year.



The main target groups for MS were either General Users or Professional Users. The number of attendees decreased compared to 2017, which may be the outcome of more targeted audience groups. The security themes covered in conferences organized in 2018 included subjects such as IoT, Practice Basic Cyber Hygiene, Expand your Digital Skills and Education, Recognise Cyber Scams, Cyber security training, and Emerging Technologies and Privacy. Feedback from attendees was positive. Remarks highlighted that the attendees favoured activities that included greater interaction (e.g., Capture the Flag, interactive sessions) and appreciated targeted content and training.

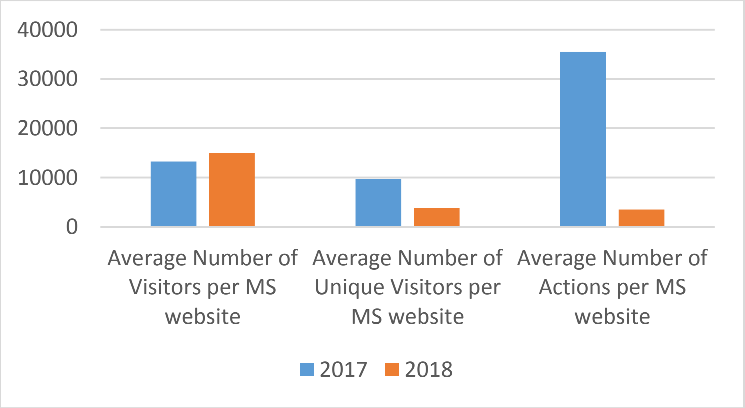
5.1.2 Results for TV or Radio Advertisement activities

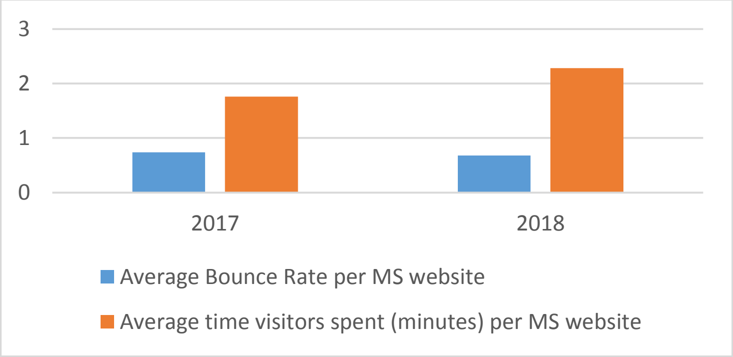




Overall only few countries implemented TV or radio advertisements in 2018. Approximately 10 TV channels and radio stations were employed to advertisements with.

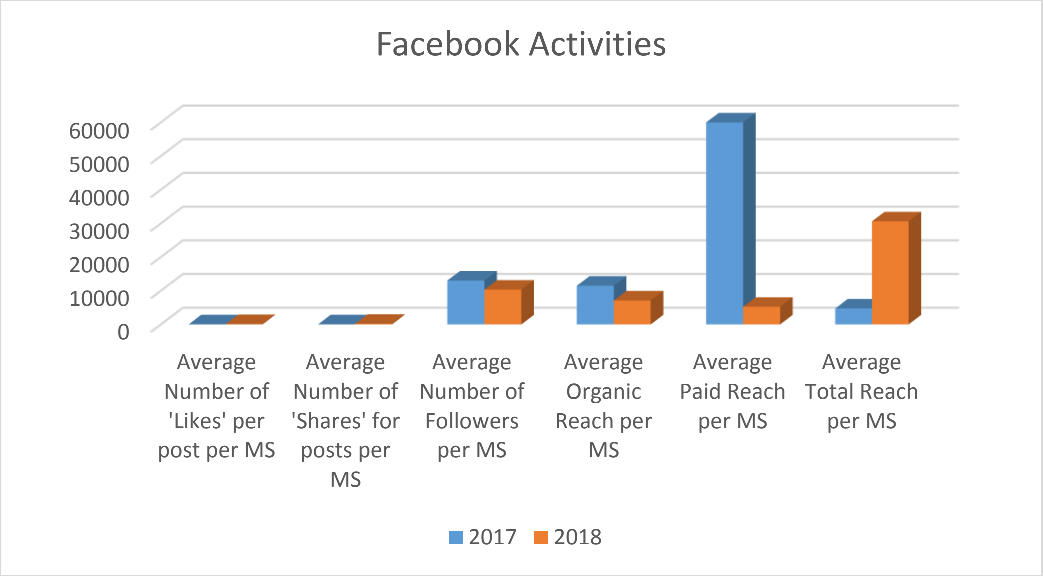
5.1.3 Results for MS Websites



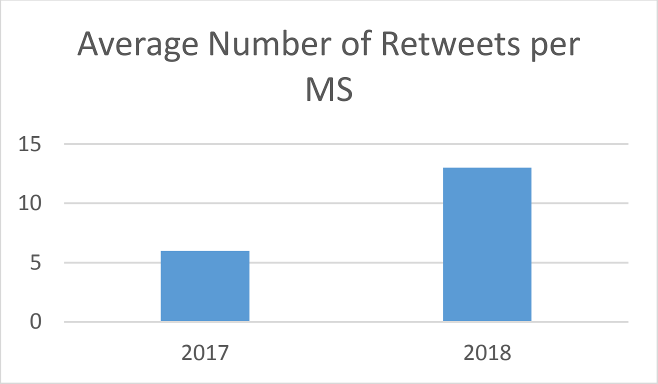


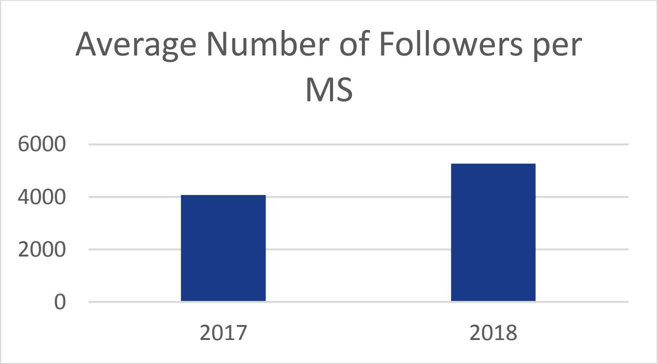
The average number of visitors increased year on year however the average number of actions per user per MS were a lot lower than the previous year. Average bounce rate and time visitors spent per MS website increased year on year.

5.1.4 Results for Social Media Activities

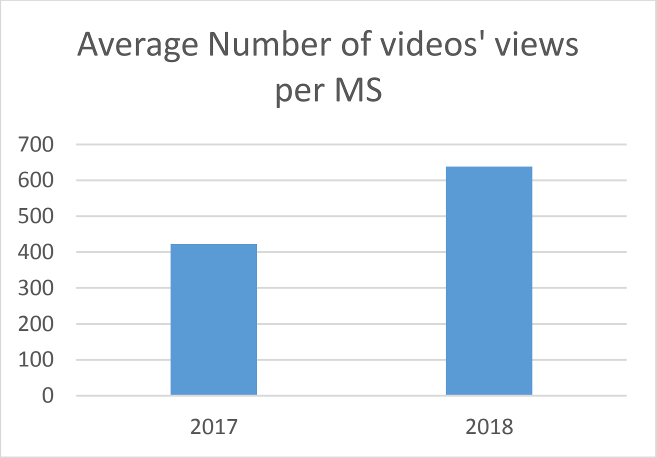


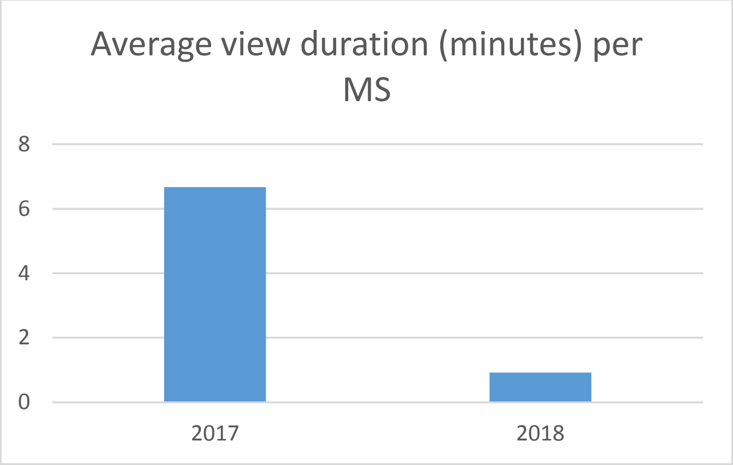
ECSM activities employed by Facebook accounts are widely popular. The figures displayed above represent the activities that took place during October 2018 for MS related accounts and posts. On average the MS coordinators reduced the paid Facebook activities, while maintaining same amount of Followers, Likes and Shares, with 2017.





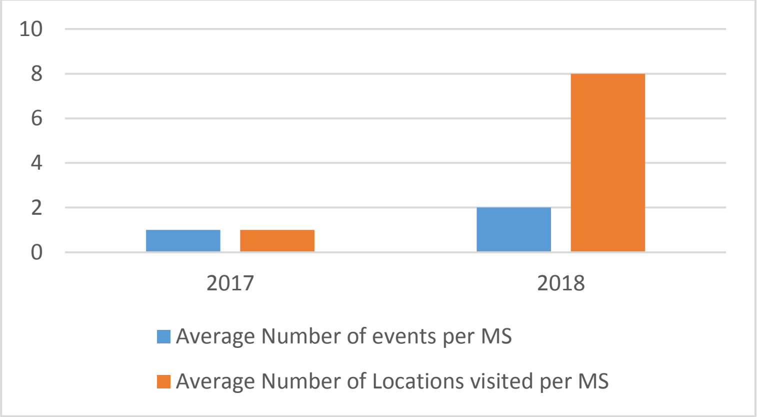
Twitter activities were more effective in 2018 and contributed to the activities with almost 5000 average number of followers per MS, and 12 retweets on average per post.

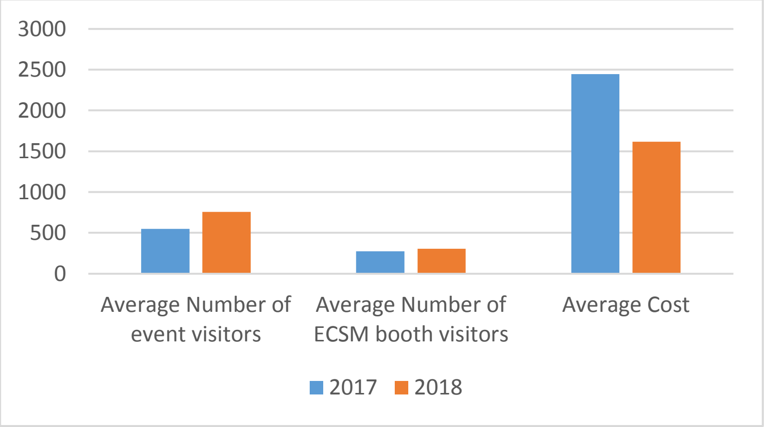




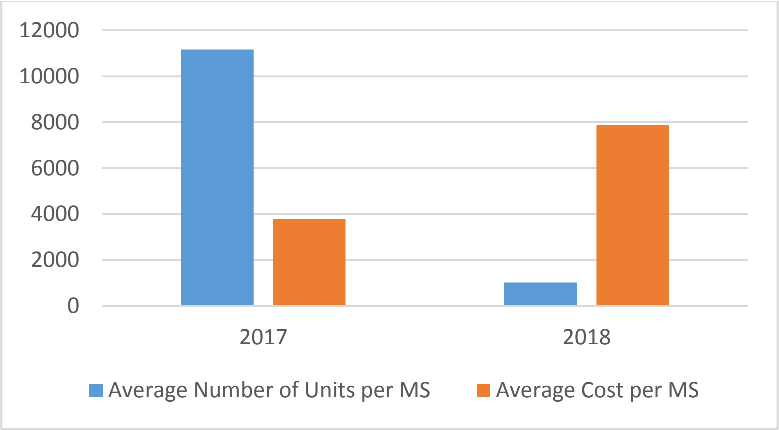
Finally some countries used YouTube channels and videos demonstrating an average number of almost 700 views per video.

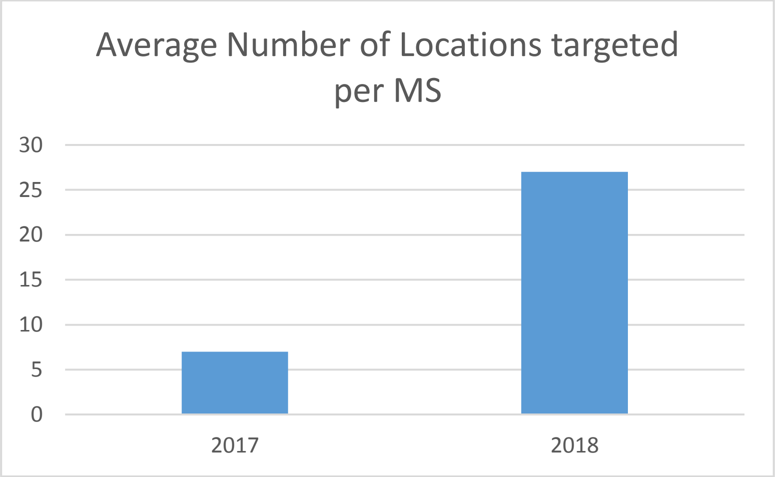
5.1.5 Fair Stand/ Exhibition and Roadshows





5.1.6 Merchandising, Posters, Leaflets





5.1.7 Tests/Quizzes

The implementation of Tests/Quizzed was less frequent in 2018. Belgium implemented a Quiz, which was taken by 15000 individuals. Hungary also implemented a Quiz which was taken by 334 individuals.

5.1.8 Organizational effort

The participating MS reported that at least one full time employee in their organization worked on the preparation and execution of ECSM 2018; one to three employees were occupied in the planning and execution, with average 55 person days fully dedicated.

5.1.9 Overall results and conclusions

The assessment included in this chapter represents the first attempt in ECSM for a systematic and comparative analysis of the ECSM activities across the Member States. ENISA developed an evaluation strategy which was communicated and agreed among the MS coordinators. The objective of this effort is to collect adequate information from the MS coordinators regarding the activities they organize during ECSM each year and analyse them to produce useful findings for the future ECSM organizations.

This report includes the analysis of the data for 2017 and 2018, with a perspective on the average measures per Member State participating. The findings are divided per category of activity. Regarding the organization of conferences and workshops within ECSM, the results showed an increased number of activities in 2018 compared to 2017 and a decreased average number of attendees; the data reflects a different approach by the MS coordinators to organize smaller events with targeted audience groups compared to 2017 in which larger events were organized for more general audience. Further, there was a significant increase on the use of advertisements in 2018 (the average number of advertisements per MS was increased four times). Similarly, the activities of roadshows, fair stands and exhibitions were significantly increased in 2018 in terms of number of visited events, visited locations, and reach. The impact of the activities through websites, Facebook and YouTube was relatively the same. LinkedIn was not popular in both periods. On the other hand, Tweeter activities were boosted in 2018 with increased number of followers and retweets. Finally, MS coordinators reported that it is difficult to estimate the cost of organization for activities, particularly because most activities are co-organized.

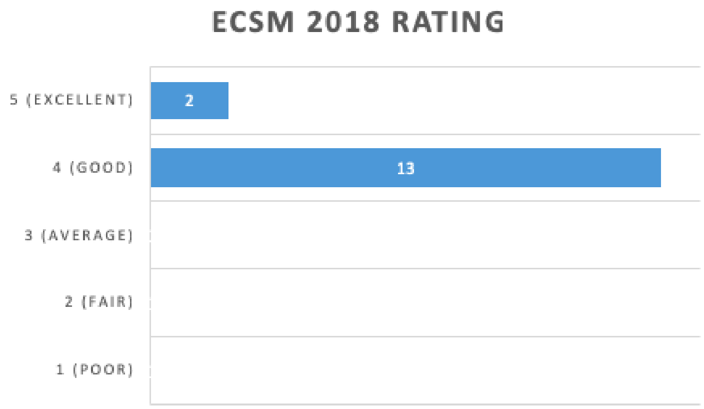
Finally, a limitation on the findings of this assessment is that the MS that participate in ECSM are commonly variant among the years, making the results less comparable however this will be remedied in future years.

5.2 ECSM Campaign Survey Questionnaire

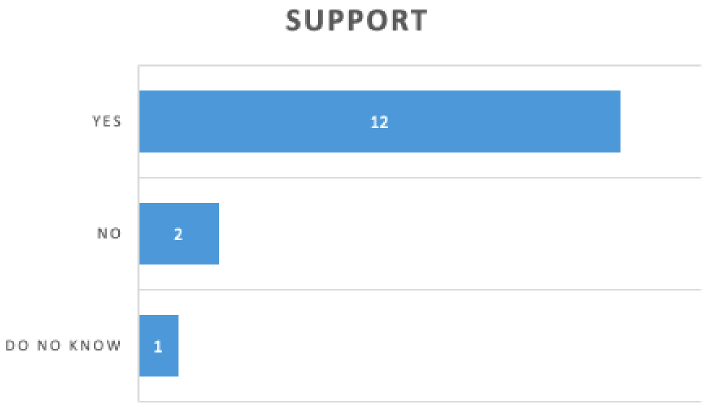
The questionnaire is an important tool used to gather the opinions of the MS coordinators that are engaged in the campaign. The charts below present the replies of 15 participants representing their MS. An increase of 3 participants compared to the previous year.

5.2.1 Member States replies

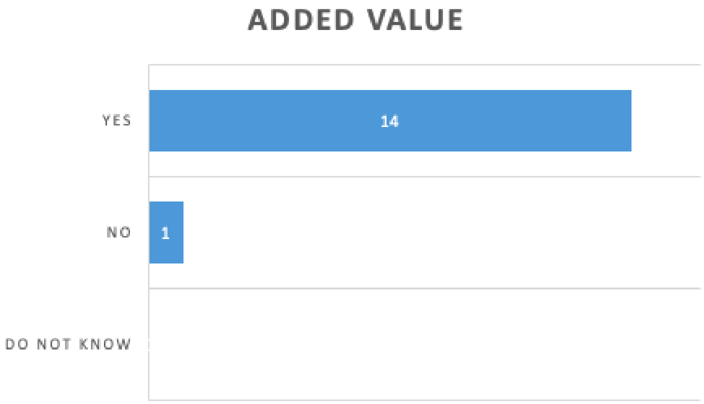
1. How would you rate the overall implementation of the ECSM 2018 campaign (scale 1-5)?



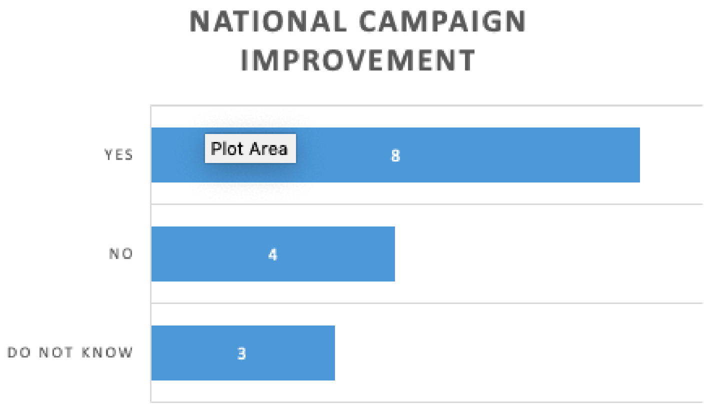
2. Did ECSM support in a satisfactory manner the outreach and promotion of your work?



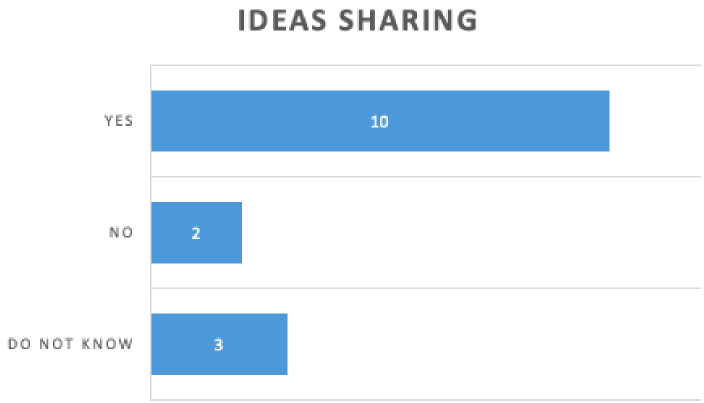
3. Did ECSM add value to your national campaign?



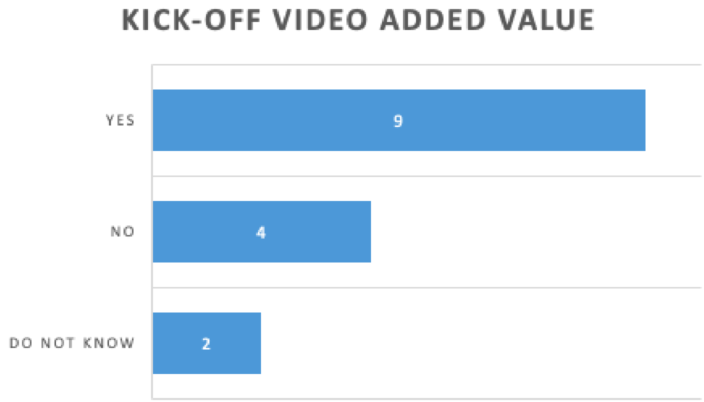
4. Did ECSM offer opportunities for improving your national campaigns through collaboration with other Countries?



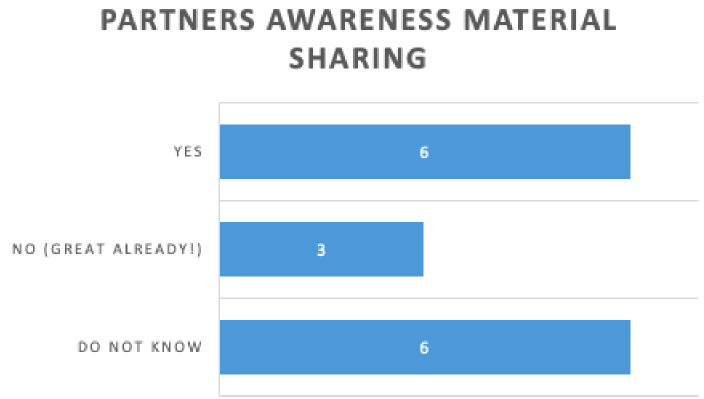
5. Do you think ENISA succeeded in the sharing and promotion of new ideas among ECSM partners?



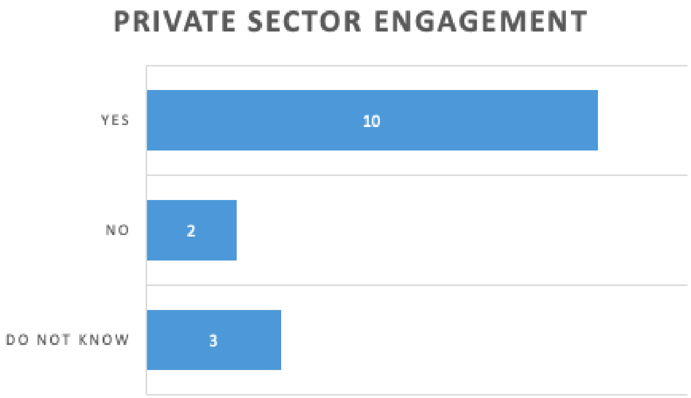
6. Did the kick video clip produced for ECSM support your national campaign?



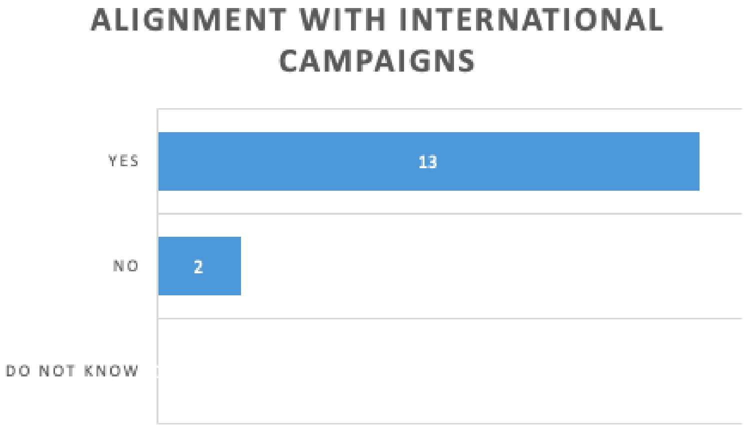
7. Could ECSM better promote the awareness material produced by its partners' campaigns?



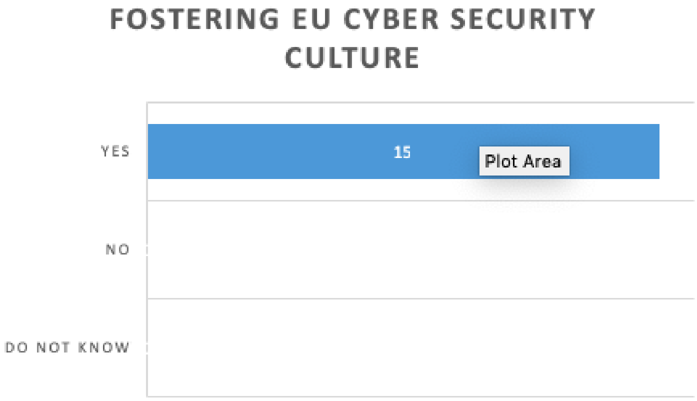
8. Would you want ENISA to facilitate in the engagement of the private sector in future campaigns?



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



10. Do you think that ECSM offers opportunities for fostering a pan-European cyber security culture?



5.2.2 Consolidated results

MS coordinators valued the implementation of campaign to be good and above based on the results of Q1. This result is slightly better than last year's results as all answers are marked as positive.

Again this year, the overwhelming majority of MS coordinators agreed that the campaign added value to their work, and that it supports their local national campaigns throughout the promotion of their work (Q2 and Q3). Two partners have encouraged the ECSM campaign to use available communications channels more efficiently (e.g., twitter, Facebook) and to better promote partners' produced awareness materials.

The majority of MS coordinators (66,6%) are convinced that the campaign offered opportunities for collaboration and sharing of ideas among the MS and only the 13, 3% believes that this is not the case (Q4). On the other hand 53, 3% believe that ECSM offers opportunities for improving the national campaigns through collaboration with other countries, while a 26,6% believes it does not (Q5).

Feedback on the added value of this year's ECSM kick-off video clip was positive from the majority of partners. 60% believe that the video clip successfully supported the national campaigns, while only a 26, 6% thought otherwise (Q6). 40% of MS coordinators denoted that the ECSM could do better in promoting the MS awareness material (Q7). The feedback for better promotion of material included the following suggestions on how this could be achieved:

- Use additional channels to promote national campaigns' awareness material, such as Facebook, in addition to existing ones as it is the ECSM website and twitter
- Awareness material and core messages should be promoted with more graphical/video content and in all languages
- Awareness messages should be more charming/funny and thus more attractive to the target audience
- Use the ECSM communication Tools (social network, website etc.) to support the national campaigns on the basis of the 2018 infographics per countries
- Use the coordination skills of ENISA to facilitate common projects involving ENISA and numerous Member States
- Place a greater effort and interaction in twitter to supporting the Member States' campaigns ("liking" and more "sharing")

Feedback related to the private sector's engagement in future campaigns was positive amongst 66% of the participants however 34% rejected or hesitated to respond (Q8). A suggestion from a MS coordinator was that this should be discussed in a future ECSM meeting amongst the MS:

"It is good to have the private actors involved, as they can reach a greater audience, however the engagement of private actors should remain a decision taken at the national level. Each member state has a différent organization and rules to integrate the private sector in its campaign."

Finally, the majority of MS coodinators were positive about the prospect of aligning ECSM with international campaigns at 86,6% (Q9) and all MS coordinators fully supported the ECSM campaign for offering more and more opportunities for fostering EU-wide cyber security culture (Q10).

5.3 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.

5.3.1 ECSM Web Page

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

- Page views: 99,057
- Website visits: 27,100
- Downloads: 1,538

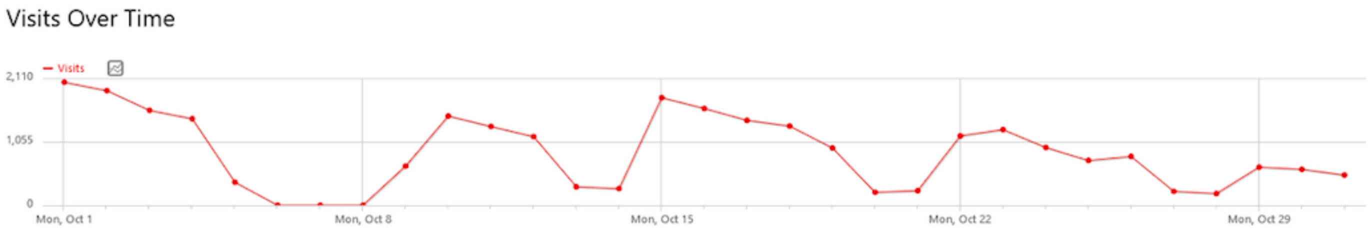


Figure 10: Graph overview of ECSM web site visits in October 2018.

Below is a comparison between this year's campaign and previous years with respect to the number of page views to the ECSM webpage. Statistics demonstrate that the ECSM website achieved stable growth in 2018, post the above average growth for 2017.

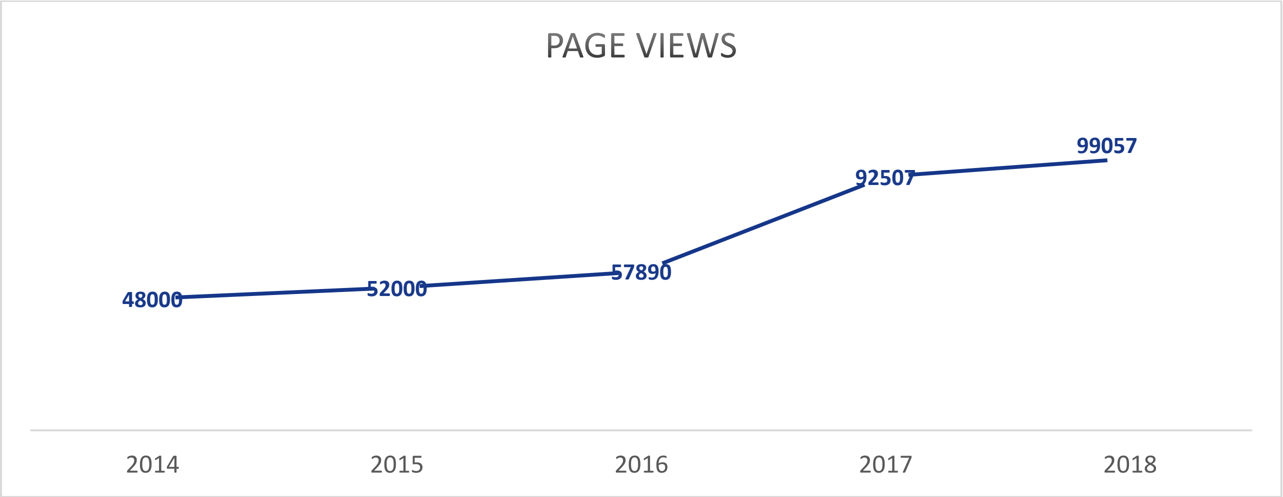


Figure 11: Overview of annual increase of ECSM page views

5.3.2 NIS Quiz

The total number of NIS Quiz page views for this year's campaign reached 62,997 views out of a total of approximately 142,294 views to the web site, which took place in the period from 1st September to 15th of November. Within 1st to 31st of October 2018, the total number of page views reached 15,191, a small decrease from the previous year. These statistics demonstrate the popularity that the NIS quiz has gained during the campaign, equating to approximately 17,6% of the total ECSM website traffic.

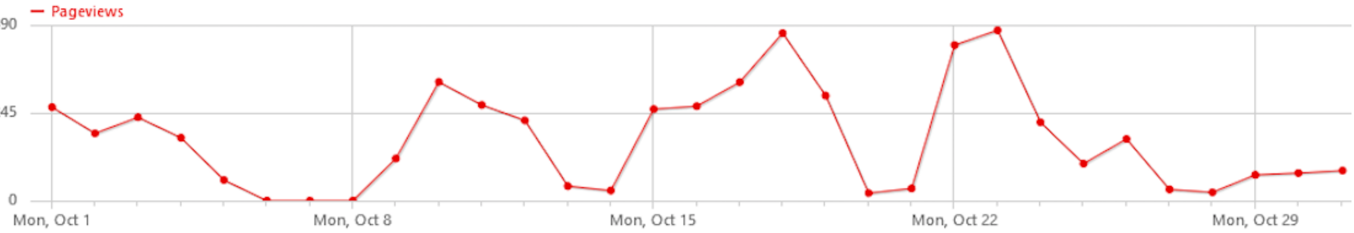


Figure 12: NIS quiz page views within ECSM October's events.

The 62,997 views of the NIS Quiz from 1st September to 15th of November can be further broken down between the views to the main page and the introductory video of the quiz as follows:

- 28,507 page views were dedicated to accessing the main NIS Quiz page
- 6,040 page views were dedicated for accessing the introductory YouTube video of the quiz

The total number of visitors succeeding to complete the NIS Quiz during month October and compared to previous years decreased from 2392 in 2017, to 1,822 in 2018. This year's statistics have also shown that from a total number of 15,191 visits to the main NIS Quiz main page, only 1,822 visitors eventually managed to complete it, a total of approximately 12%.

5.3.3 ECSM Map of Activities

The images below illustrate the number of events taking placing in October and the number of Member States / EFTA countries and other European countries organizing activities. The left hand side graph presents the total number of events registered each year from 2014 to 2018. On the right hand side, the number of EU countries for which at least one event is registered for the same period, is also illustrated.

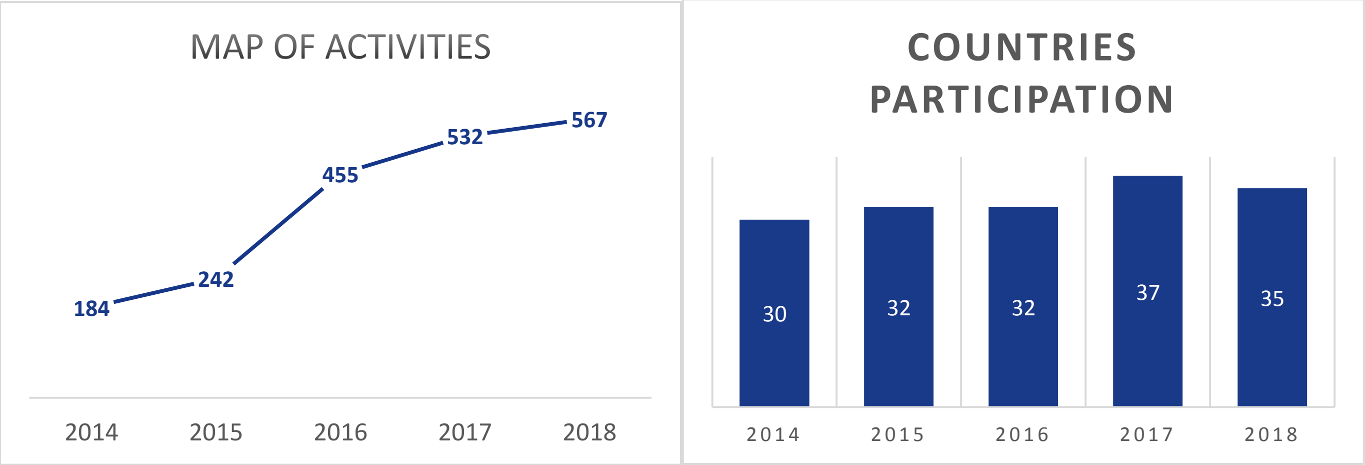


Figure 13: Number of activities in October and the number of countries registering activities annually

The rate of growth in 2018 has shown a stable increase of submitted events since previous year's campaign. A stable growth rate of events year on year were recorded from inception up until 2015, wherein the number of events registered almost doubled in 2016. The growth in the number of events registered is an outcome of the increased popularity of the campaign, which grows steadily on a yearly basis.

The top ten MS with respect to the number of events registered during October are displayed in the pie charts below for 2017 and 2018. A notable difference from last year's campaign is Poland and Hungary, that are now included in the top 5 MS with the most number of registered activities.

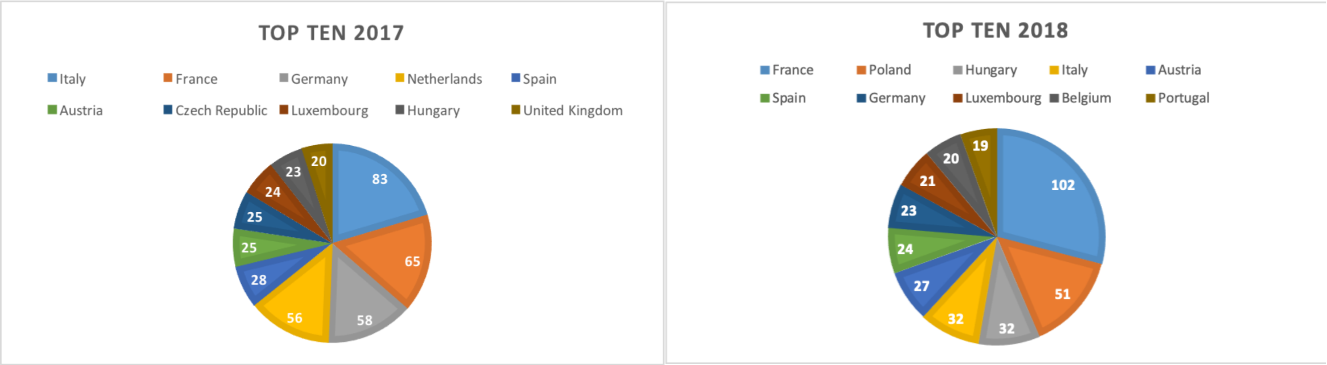


Figure 14: Top Ten countries with respect to the number of events registered for ECSM 2017 and 2018

5.3.4 Social Media

Twitter continues to support the promotion and outreach of the campaign. The figures below demonstrate the fluctuation of twitter followers from September until November 2018 for the handle *@CyberSecMonth*. The highest peak corresponds to the launch of ECSM and specifically the Kick-off event on the 1st of October, followed by renewed interest again until the latter end of the month.

Useful statistics that are extracted from the graph are:

- The total number of followers reached 16,500
- The amount of 1,667 new accounts were created within this three month period

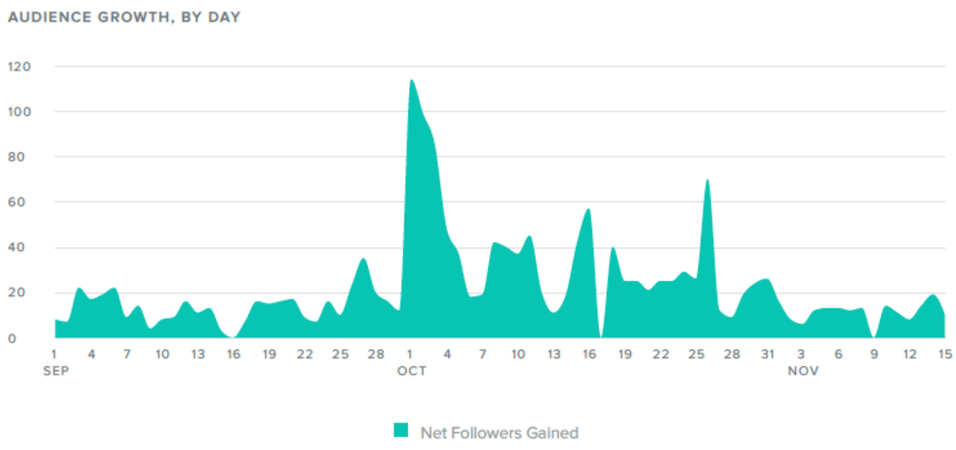


Figure 15: The daily growth of Twitter followers from September to November 2018 to @CyberSecMonth

The graph below tracks the growth in the number of twitter followers of @CyberSecMonth over time. It shows an accelerated growth also in this year's 2018 campaign.

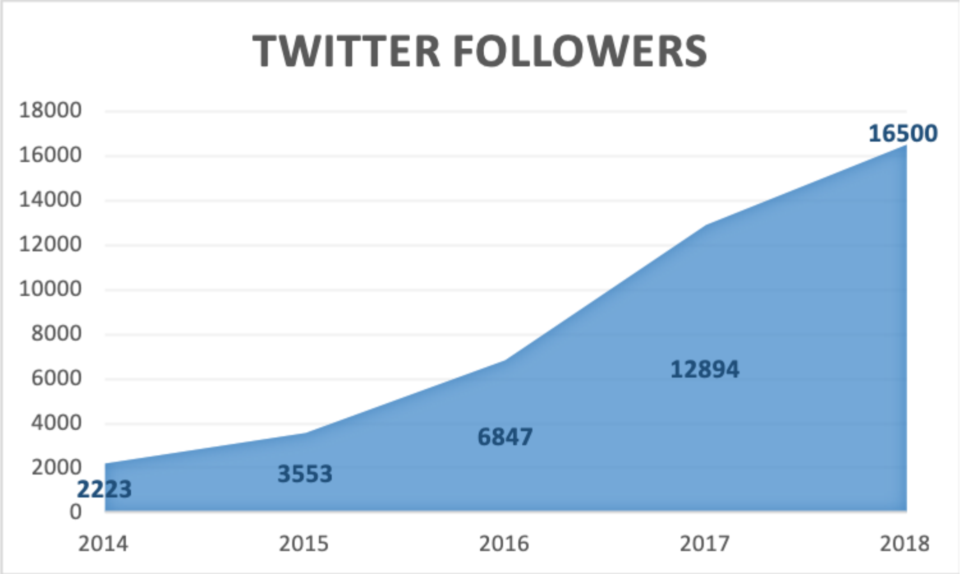


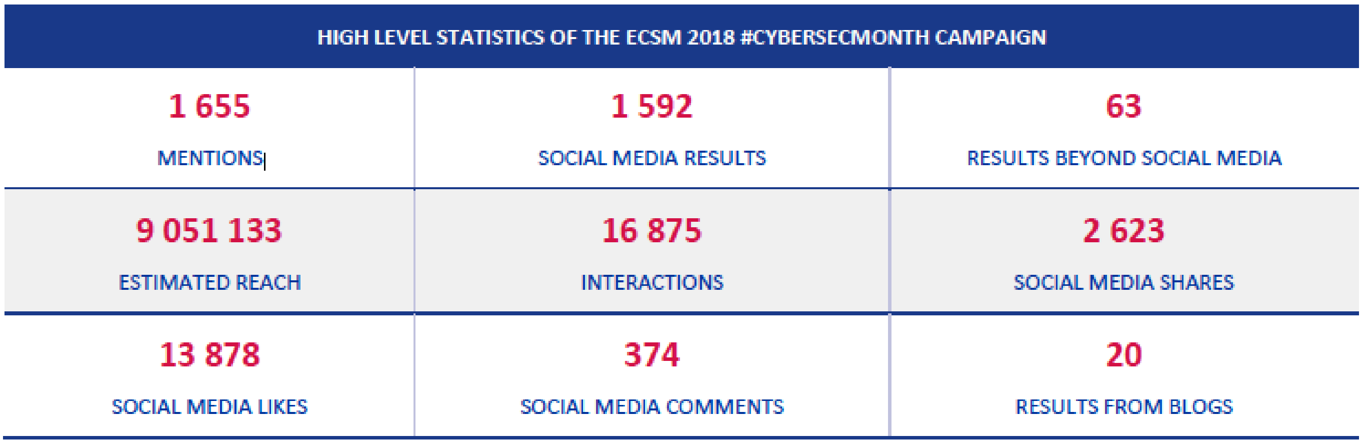
Figure 16: Annual number of Twitter followers @CyberSecMonth

5.3.5 Media Reach

The European Cyber Security Month (ECSM) project was supported by an impactful Digital Public Affairs cross-channel campaign led by the hashtag **#CyberSecMonth**. The statistical results of the campaign demonstrate a stellar online impact endorsed by a remarkable amount of mentions, reach and social media interactions.

A total number of **1655 articles** that mention ECSM from the period 24th of September till the 9th of November have been recorded with a total estimated reach of **audience exposed of 9051133**. The majority of #CyberSecMonth mentions were created on Twitter (829) and Instagram (351), followed by Facebook (313) and traditional blogs (20).

The following statistics provide in-depth insights into the impact of the #CyberSecMonth campaign, and the general exposure of the Digital Public Affairs campaign supporting the European Cyber Security Month.



HIGH LEVEL STATISTICS OF THE ECSM 2018 #CYBERSECMONTH CAMPAIGN		
1 655 MENTIONS	1 592 SOCIAL MEDIA RESULTS	63 RESULTS BEYOND SOCIAL MEDIA
9 051 133 ESTIMATED REACH	16 875 INTERACTIONS	2 623 SOCIAL MEDIA SHARES
13 878 SOCIAL MEDIA LIKES	374 SOCIAL MEDIA COMMENTS	20 RESULTS FROM BLOGS

Table 3: High level statistics of ECSM 2018 for the #CYBERSECMONTH campaign

The following table indicates the amount of mentions and reach of the top 15 countries in context of the #CyberSecMonth campaign. These statistics are estimations based on geolocation of IP addresses.

#	COUNTRY	MENTIONS	REACH
1	United Kingdom	135	75 614
2	United States	69	66 674
3	Belgium	66	66 492
4	Romania	49	8 053
5	France	43	7 553
6	Norway	25	2 071
7	Italy	24	26 228
8	Spain	22	100 761
9	Malta	16	4 941
10	Sweden	16	1 943
11	Ireland	15	13 501
12	Germany	7	330
13	Canada	7	319
14	India	6	15 730
15	Poland	6	1 852

Table 4: Amount of #CYBERSECMONTH campaign mentions per country in world-wide scale

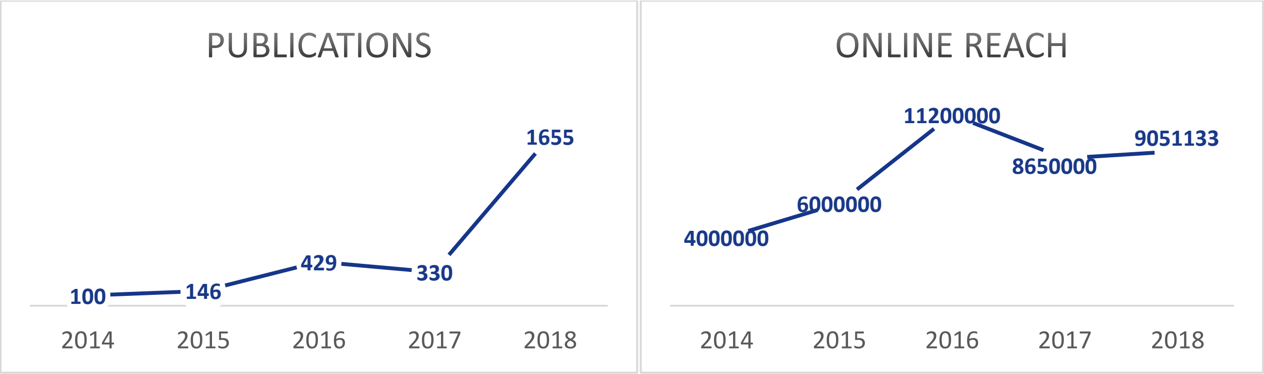


Figure 17: A comparison overview of the campaign's number of articles published and online reach in years 2014-2018.

5.3.6 Get Cyber Skilled Campaign data

'Get Cyber Skilled' eTwinning learning event came to a close on 22 October.

- 164 teachers coming from 22 countries took part in the online event consisting of five different modules. ¾ of the participants received the final course certificate.
- While the post-event evaluation survey is still open, preliminary results show that 58 per cent of respondents regard the Learning Event as "excellent" while 41 per cent considered it to be "very

good", and 70 per cent declared they will be using the acquired skills and information in their teaching activities.

- On social media, the #GetCyberSkilled hashtag received extremely good coverage as demonstrated by the Union Metrics tracker stats which show that it obtained a potential 1.8 million impressions since September 2018. (Source Twitter Analytics).
- The most successful media tweet this month was related to the #GetCyberSkilled Learning event which earned over 100 engagements. (Source Twitter Analytics).

5.3.7 Conclusions

The majority of the indicators used to evaluate the campaign demonstrate a higher growth rate year on year. For this year, a linear growth has been noticeable with respect to the rate of Twitter followers, the ECSM web page views, ECSM map of activities, the campaigns online reach, while a rather substantial increase on the articles that mention ECSM was recorded. Some analytics did demonstrate a small decrease in comparison to previous year such as the NIS quiz page views and completion attempts.

Conclusively, the increase of the ECSM campaign's popularity is visible in all numbers, contributing towards an indisputable higher performance in comparison to all previous years, leading to a successful campaign also for ECSM 2018.

6. Conclusions

The evaluation of the campaign is based on the analytical data gathered, the feedback received from MS coordinators and for the first time the use of evaluation metrics data from the base year of 2017. The campaign continues to grow in line with expectations and the long term growth rate. Several of the factors that contributed to the success of the campaign in 2018 were:

- the increased commitment by the Member States towards awareness raising,
- the "Get Cyber Skilled" campaign supported by the European Commission, European Schoolnet and SaferInternet4EU campaign,
- the awareness campaign executed by EC3 & EBF related to "Cyberscams"
- and outreach using social media channels.

In the ECSM deployment report of 2017 a number of observations were made by ENISA to support the success of the campaign going forward. These observations are revisited below and include updates on how they were addressed during the year.

6.1.1 Evaluation metrics

This was the second year that evaluation metrics were collected from the MS and resulted in the first year a comparison could be drawn from previous year's results to evaluate the campaigns progress. The number of Member States contributing to the evaluation metrics increased from seven in 2017 to ten in 2018, however only three countries reported in both years. Although the results are averaged per MS, comparable results will only be achieved once all MS are providing comprehensive metrics year on year.

6.1.2 Member State Commitment

The core campaign coordinators participating actively in the monthly conference calls and physical meeting increased with the addition of Belgium and Malta.

Member States & EFTA countries actively participating in the campaign include: Austria, Belgium Czech Republic, Estonia, Finland, France, Germany, Hungary, Luxembourg, Malta, Netherlands, Norway, Portugal Poland, Romania, Slovenia, and Switzerland.

6.1.3 Private Sector Involvement

The private sector continued to show much willingness to contribute to the campaign. The structure and form of such an engagement remains to be decided by the MS.

6.1.4 Governance Structure

The proposal for the introduction of a governance structure was a moot point for some of the MS during the physical meeting in Brussels. Concerns raised included obligations, responsibilities, keeping deadlines and loss of flexibility if a governance structure was in place, whilst for others considered a governance structure as overkill given that there is not budgetary decisions to make.

6.1.5 Collaboration with the European Commission

There was a step up in collaboration with the European Commission during the run up to October. A number of significant steps were taken to cross promote each other's efforts. The first being the saferinternet4EU campaign for which ENISA supported with the Get Cyber Skilled campaign during week two and the second being the award of European Schoolnet competition for which the ENISA Executive Director was Ambassador.

6.1.6 Annual ECSM Launch Event

It was decided during the physical meeting in Brussels with the MS that the annual kick-off event to launch the campaign will be replaced by a kick-off video featuring the MS with messages and a call to action. The video included messages from seven MS in their local languages and also a message and call to action from the Commissioner Mariya Gabriel.

As of the December 2018 the kick-off video has had over 1500 views in the space of two months that will continue to grow over time. If we are to compare the amount of viewers of the video with the amount of participants present at the 2017 annual ECSM kick-off event in Tallinn, the outreach of the video is tenfold. Thus the decision to use video as a medium to reach out to European citizens has been vindicated by the numbers; however much work is needed to reach the millions of citizens of Europe.

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

TP-03-18-556-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-280-6
DOI: 10.2824/0844