EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUROPEAN CYBERSECURITY MONTH (ECSM) 2020

Deployment Report

APRIL 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, please visit https://www.enisa.europa.eu

Contact

To contact the authors, please email ecsm@enisa.europa.eu
To contact the media office, please email press@enisa.europa.eu

Legal notice

Copyright notice

ISBN: 978-92-9204-466-4
ISSN: 2600-0571
DOI: 10.2824/224495

EXECUTIVE SUMMARY

The EU Cybersecurity Act (CSA) came into force on 27 June 2019 with an emphasis on making cybersecurity a priority in awareness campaigns. In accordance with Articles 4 and 10 of the CSA, the European Union Agency for Cybersecurity (ENISA) must promote a high level of cybersecurity awareness, including cyber hygiene and cyber literacy among citizens, organisations and businesses.

Since 2012, the Agency has been raising public awareness of cybersecurity risks through an annual EU-wide awareness-raising campaign aimed at citizens, organisations and businesses – the European Cybersecurity Month (ECSM). The month-long campaign every October across Europe, and beyond, promotes cybersecurity awareness and education, and provides guidance on good practices for individuals and organisations in order to create a more cyber secure culture across the EU and increase resilience.

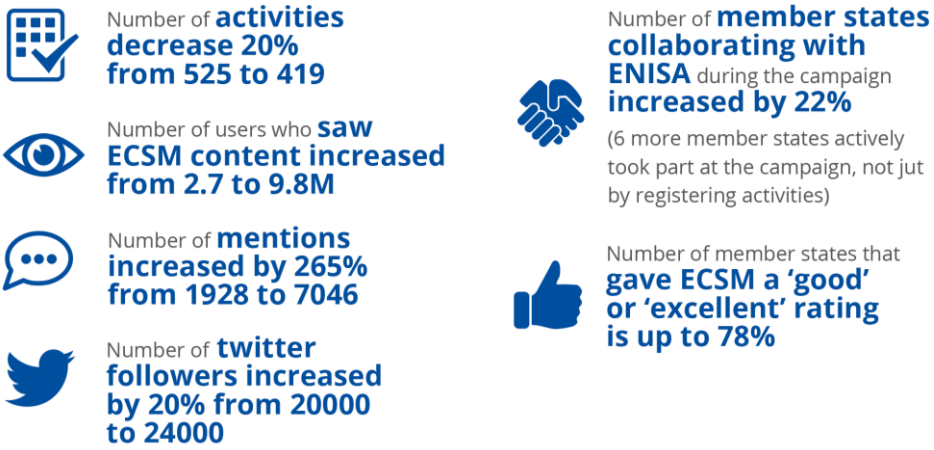
The COVID-19 pandemic changed the scope of the ECSM, but not the level of outreach or success. Every year, the ECSM has been an interactive month with in-person events spread across countries. It has been a platform for sharing ideas and campaign materials between countries. The campaign includes new collaboration, workshops, conferences, training sessions and much more. This year, the pandemic posed a great challenge, namely to transfer this platform to a digital one –for both organisers and participants.

ENISA was up for the challenge. The Agency set forth an ambitious online campaign, entitled 'Think Before U Click', with the social media hashtag #ThinkB4UClick. The action plan called for an ambassador's programme, a partnership programme and a social media programme.

The online ECSM 2020 campaign was a success, garnering three times more engagement than the previous year.

Each year, the ECSM addresses the disparity between cybersecurity practices across EU Member States.

Highlights of the 2020 ECSM Campaign



This report provides an overview of the activities organised and presents a synthesis of the findings based on evaluation and performance information gathered via two questionnaires, a social media monitoring report, and media and social monitoring reports. The two questionnaires were based on two surveys provided to the Member States and were used to measure the overall performance of the ECSM campaign and the individual national campaigns based on given evaluation metrics.

The ECSM deployment report is structured into an introduction and three phases: (1) planning, (2) execution and (3) evaluation.

The introduction provides readers with the policy context, scope and target audience for the campaign. The planning phase describes the key design elements for the activities that took place during the ECSM and that facilitated the work of Member State and EFTA countries' coordinators. This includes how events were organised and coordinated with coordinators, as well as decisions on the marketing materials and channels used. The execution phase of the report highlights the milestones achieved and insights into the execution of the campaign. The final section of the report deals with the evaluation of the campaign, comparing results from this year with previous years through an evaluation metrics survey. This survey is used by Member States to measure the performance (activities, social media, etc.) of their national campaigns and in each year. ENISA receives the data from this survey and uses them to compare this year's performance with previous years' results based on the same metrics.

The report concludes with recommendations to establish a governance structure to support the decision-making of the outreach programme and to maintain the campaign's engagement with EU citizens throughout the year (in addition to the campaign focus for the month of October).

The ECSM deployment report is intended to provide a basis for discussion among 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 continue engaging citizens and organisations in boosting cybersecurity awareness and education.

TABLE OF CONTENTS

1. INTRODUCTION

The European Cybersecurity Month (ECSM) is the EU's annual campaign dedicated to promoting cybersecurity among citizens and organisations and to providing up-to-date online security information through awareness raising and sharing of good practices. Each year, for the entire month of October, hundreds of activities take place across Europe, including conferences, workshops, training sessions, webinars, presentations and more, to promote digital security and cyber hygiene.

The ECSM campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission and is supported by EU Member States and hundreds of partners (governments, universities, think tanks, non-governmental organisations (NGOs), professional associations and private-sector business) from Europe and beyond.

ENISA coordinates the organisation of the ECSM campaign by acting as a 'hub' for all participating Member States and EU institutions, and by providing expert suggestions, generating synergies and promoting common messaging among EU citizens, businesses and public administration. The Agency also publishes new materials and provides expert advice on different cybersecurity topics for Member State audiences.

'Cybersecurity is a shared responsibility'

Since the first event in 2012, the ECSM campaign has been meeting its key priorities by bringing together parties from across Europe under the slogan 'cybersecurity is a shared responsibility' to unite them against cyber threats. Each year, not only does the campaign promote the safer use of the internet for EU citizens, but the organisers provide the knowledge and tools to do so.

Awareness raising is an indispensable component of improving cybersecurity within the EU. However, the scope of this challenge is huge. With some 95 % of incidents said to be enabled by 'some type of human error – intentional or not' ([1]), there is a strong human factor at play, making cybersecurity everyone's responsibility. This means that personal, corporate and public administration behaviour must change to ensure that 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 ECSM under the coordination of ENISA is one of the mechanisms by which cyber hygiene and awareness is promoted among the citizens and businesses of Europe. The ECSM runs for the entire month of October, with ENISA publishing new material and focusing on different topics throughout the month.

This report summarises the activities carried out by ENISA and the participating Member States for the 2020 campaign and presents the evaluation and conclusions of the campaign. More importantly, it seeks to trigger a discussion among Member State coordinators with respect to future improvements.

([1]) *IBM Security Services 2014 Cyber Security Intelligence Index.*

1.1 PURPOSE AND GOALS

The scope of this report includes all of the activities within the ECSM campaign and their impact in 2020.

The purpose of the ECSM project is to increase end users' resilience in cybersecurity across the EU. Therefore, the main goals of the ECSM 2020 campaign were as follows:

- generate general awareness about cybersecurity;
- educate and enhance awareness of information security and privacy by increasing awareness of cyber scams and digital skills;
- promote the safer use of the internet for all users and the practice of basic cyber hygiene;
- continue building on the strong track record of this annual campaign in raising awareness of cybersecurty across Europe;
- engage relevant stakeholders and increase the participation of EU Member States;
- increase media interest at EU and national levels through a Europe-wide campaign and through national campaigns;
- boost attention and interest with regard to information security through political and media coordination.

1.2 EVALUATION METHODOLOGY

In 2017, ENISA developed an evaluation strategy to guide the Agency and Member States in gathering data and information for the evaluation of the campaign. The same evaluation strategy was employed in 2018, 2019 and 2020. Member State coordinators were urged to consider and define the evaluation metrics during the planning stage of the campaign so that the correct data and information would be collected during the execution stage.

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

- a collection of quantitative data from Member State campaign coordinators;
- feedback from Member State campaign coordinators via the end-of-year questionnaire;
- the use of social media and media monitoring services to gather analytical data.

An evaluation data collection form was developed by ENISA in collaboration with Member State coordinators for information gathering. The evaluation form aims to collect participant feedback, extract pertinent information and identify the potential impact overall on the activities involved in the Member State campaigns. The evaluation form was distributed to Member State and EFTA countries' coordinators in the form of an online survey, using the European Union platform EUSurvey (https://ec.europa.eu/eusurvey/). The Agency requested that coordinators complete their surveys based on their national campaign strategy and execution. The data collection form was accompanied by guidelines that highlighted the recommended metrics for each type of activity.

The evaluation strategy also included a questionnaire, the aim of which was to extract information on the implementation of the campaign based on the feedback from Member State campaign coordinators with respect to the Agency's supportive role. Some of the elements that were assessed included the level of support and its usefulness to Member States, the impact of promotional materials that were used and marketing strategies that were followed, and the role of the ECSM in improving the outreach of Member State campaigns (for more information, see Section 4 of this report).

1.3 TARGET AUDIENCE FOR THIS REPORT

This report is intended for organisations (public or private) that have supported the ECSM or intend to do so in the future. The report may also be of interest to information technology (IT) security professionals and other target groups who have attended ECSM events. Furthermore, the report targets EU national policymakers who are aiming to improve the security awareness of citizens, professionals and, more generally, IT end-users.

2. PLANNING PHASE

2.1 ROLE OF ENISA IN ECSM 2020

2.1.1 Vision statement

Through the ECSM, ENISA supports EU Member States in the design and implementation of their awareness-raising campaigns, coordinates the campaign at the EU level and promotes collaboration among Member States, international organisations and industry to increase resilience in cybersecurity among EU citizens and organisations. It also aims to create a cyber secure culture across the EU. ENISA does so by collaborating closely with the European Commission and Europol.

2.1.2 Mission statement

The Agency's mission for the ECSM is to collaborate with the EU institutions, Member States and international organisations by finding innovative and fun ways to raise EU citizens' awareness of cybersecurity and enhance the pan-European vision of stronger cybersecurity.

2.1.3 Objectives for ECSM 2020

Participating Member States reached a consensus on defining the Agency's objectives for the ECSM. The objectives were as follows:

- promote the underlying value that is the foundation of the ECSM, namely that cybersecurity is a shared responsibility;
- assist Member States in implementing ECSM activities that satisfy certain criteria, namely activities that have well-defined objectives, well-specified target audience(s) per activity, systematically defined cybersecurity subjects, systematically chosen delivery channels and techniques, and well-defined effectiveness metrics;
- support Member States in defining common areas of concern for cybersecurity that will be promoted to EU citizens by all Member States.

ENISA supported the organisation of the ECSM campaign in various ways, including by:

- coordinating and organising the ECSM;
- acting as a 'hub' for all participating Member States;
- collecting available materials from and boosting synergies between Member States;
- acting as a subject matter expert on how to organise information security campaigns and on how to design the content and evaluation strategy for information security campaigns;
- facilitating common messaging within the participating Member States by providing tips and advice on how to be safe and secure online;
- creating the ECSM brand and related communication plan;
- distributing promotional material.

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

2.2 COORDINATION

2.2.1 Conference calls

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

The Agency prepared the meeting agenda before each conference call. Meeting minutes were drawn up by ENISA after every call and included a list of action points. The participation rate was high, with an average of 21 to 25 participants per meeting.

2.2.2 Planning meeting

In March 2020, the Agency organised an in-person meeting in Brussels, where Member State and EFTA countries' coordinators were able to discuss both their concerns and opportunities for improvements, as well as finalise key areas of the campaign, such as the themes of the month, the collaboration infrastructure, the organisation and the activities. Owing to the COVID-19 pandemic, the other planned coordination meetings took place via conference calls.

2.2.3 Themes of the month

At the March 2020 meeting in Brussels, the Member State coordinators also discussed and agreed on the benefits of designing their campaigns around commonly agreed security and privacy themes.

One of the main agenda points of the meeting was the discussion of how to organise the themes of the month. The decision was to continue with two themes over the month, as in 2019.

With regard to the themes, after discussions about threats and their corresponding mitigating actions, the themes were consolidated into broad, all-encompassing topics.

The group identified the following themes for ECSM 2020:

- **Cyber scams – weeks 1 and 2**
- **Digital skills – weeks 3 and 4**

After the selection of the themes, a task force was organised for each theme in order to design the campaign around the theme, produce the content and validate the products proposed by the digital media contractor.

A total of 31 outputs were developed, which revolved around two videos and two infographics.

2.2.4 Digital material and social media development

In 2020, ENISA invested in developing extra digital material for online dissemination compared to previous years, in order to increase ECSM brand awareness, reach its target audience and increase engagement in its online channels, including Member States' and EFTA countries' platforms and the ECSM social media channels.

Within this activity, ENISA signed a communication framework contract and collaborated with an external contractor who committed to the following tasks.

- Assist in building target audience personas. This activity involved undertaking quantitative and qualitative research to get a rounded picture of the target audience personas.
- Develop new content for owned and earned media campaigns. Based on the analysis of the review, this activity included planning for the development of new content for the

owned and earned media campaigns. This included the development of videos, infographics, social media posts including short quizzes, etc.

Another contract was opened to develop three additional videos, depicting real-life situations connected to the topics of phishing and privacy.

2.2.5 Virtual launch of the ECSM campaign

The European Commission, in collaboration with ENISA, designed the implementation of a virtual event for launching ECSM with Commissioner Hahn (Inter-institutional kick-off of the European Cybersecurity Month: Combating cyber-scams in the light of COVID-19). It hosted a panel of high-level representatives of different European institutions and agencies, watched by numerous online viewers.

Furthermore, a video for the launch of the campaign was created. The video features interviews with Juhan Lepassaar, ENISA's Executive Director, and Jakub Boratyński, Head of Cybersecurity and Digital Privacy Policy of the Directorate-General for Communications Networks, Content and Technology (DG Connect).

2.2.6 Press releases

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

2.3 ECSM TARGET AUDIENCE PERSONAS

During the planning phase, the Agency identified the necessity for the execution of research to specify the ECSM target audience groups. The results of this research, which took place in collaboration with the task forces of Member State campaign coordinators, indicated that the main categories of the ECSM's target audience include, for the 'cyber scams' theme, general users, the elderly and business users and, for the 'digital skills' theme, children and young adolescents, students and young adults, parents/teachers/educators and the elderly.

2.3.1 General users

'General users' primarily refers to consumers who are 25 to 54 years old, are EU citizens who use the internet and especially online shopping services (mainly in the category of clothes and sports) and make online purchases from their country or other EU countries. Few of them have reported online fraud problems (2.5 %) and a significant percentage (25 %) have reported that their biggest barrier to making online purchases is payment security, or privacy concerns.

2.3.2 Young people

The category of young people primarily refers to secondary school pupils who are mainly motivated by social media networking and gaming. This target audience category uses platforms such as *Snapchat* and private messaging services such as *Kik*. Secondary school teachers regarding pupil privacy, including concerns about the sharing of intimate images, cyberbullying and fake news, express significant worries. A typical example of this target audience category would be a 16-year-old female pupil who lives with her parents in an urban area, browses the internet using her mobile device, is active on Snapchat, Instagram Stories and private messaging apps, and feels under pressure to share 'selfies'.

2.3.3 Business users

The third target audience category refers to small and medium-sized enterprises (SMEs) in the EU that are mainly independent (i.e. many are run by self-employed individuals). The main

industries involved are accommodation and food services, retail, business services and construction. Business users are profit driven; they are looking for efficiencies and cost reduction, as well as opportunities to grow. They are commonly characterised by limited time. A typical example of this target audience persona is a 45-year-old male who works in the technology sector, browses the internet using his laptop and mobile device, is active on Twitter and LinkedIn, and is interested in ways to save money and be more productive with time.

2.3.4 Elderly users

The fourth category concerns senior citizens who, in the midst of the COVID-19 pandemic, had to deal with the full digitalisation of all aspects of their daily social and financial life without having the necessary IT and cybersecurity education and skills.

2.4 CAMPAIGN MATERIAL FOR 2020

ENISA, the European Commission, Europol and the Member States were all committed to raising awareness in 2020. A series of marketing channels and materials were used to achieve this purpose, as presented below.

2.4.1 Visual identity

In 2020, the Agency updated the visual identity of the ECSM to introduce a more contemporary look and feel and to better engage with a wider audience. The logo ([2]) of the campaign remained unchanged, while the colour chart, the typography rules, the guidelines on the use of imagery, the design templates, the campaign's main visual and the manual of formal guidelines on the proper use of these elements were updated.

2.4.2 Slogan

The general tagline 'cybersecurity is a shared responsibility' was maintained in 2020. A motto was added for the 2020 campaign, 'Think Before U Click', with the hashtag #ThinkB4UClick actively used on social media and in the campaign's visual output.

2.4.3 Press release

The Agency wrote this year's press release with key input provided by the European Commission (Annex A) to ensure maximum outreach and to stimulate attention to the activities and events featured. The press release was translated into all of the official languages of the EU and was released on 30 September 2020.

2.4.4 Social media: Banners

The web and social media banners (Figure 1) were fully updated in 2020, based on the campaign's new visual identity. The banners (two different variations) are available in different formats to be used in different channels (i.e. Facebook, Twitter and the website). All banners are available at https://cybersecuritymonth.eu/press-campaign-toolbox/visual-identity.

Figure 1: ECSM 2020 social media banner

2.4.5 Videos

In 2020, the social media and marketing strategies contractor developed two animated videos focused on the two main themes of the campaign:

- how to avoid cyber scams,
- digital skills.

The videos were designed to be divided into smaller independent videos, as a means to maximise their dissemination on social media (YouTube was also used as a dissemination channel). The videos were translated into the participating Member States' languages (i.e. 24 languages), so that they could be used by the national coordinators in their national campaigns.

Furthermore, the Agency decided to develop three additional videos with another contractor, to depict in a different way the cyber risks associated with the main themes. Human actors were used to recreate real-life situations involving cybersecurity risks:

- be aware of phishing,
- protect your privacy online,
- online shopping.

The videos were also used during the social media campaign and were designed to be language-free to avoid translations.

2.4.6 Infographics

The digital media contractor developed two main infographics with the support of the task forces:

- stop your business being scammed,
- online financial safety.

The infographics were translated into the participating Member States' languages so that they could be used by the national coordinators in their national campaigns.

2.4.7 Stickers

In 2020, the 2019 stickers were also used.

2.4.8 Website

Following a usability evaluation survey that took place during ECSM 2019, the ECSM website ([3]) was completely redesigned, with a more modern and user-friendly layout. The landing page was re-designed to offer quick access to campaign resources and connected events, with a dedicated search function that could be filtered according to the persona identified. The redesign also meant that the resources page could be more easily navigated and the events page was moved to be displayed in a list of upcoming activities. A new section dedicated to each country's national campaign was created to highlight Member States' initiatives. All of the website's content was updated according to the new structure, but the previous years' material was also preserved. Following the website's redesign, Member State coordinators could directly manage their national sections, events, resources and more.

2.4.9 Translation of material

The Agency worked with the digital media contractor and the European Commission to translate the text of the infographics, the two main campaign videos and the press release into all of the EU languages in 2020.

([3]) https://cybersecuritymonth.eu/

2.4.10 Paid advertisement campaign

The Agency contracted a company to support the earned media campaigns by paying for social media advertisements, which were placed to ensure the content was reaching a wider audience.

2.5 EVALUATION STRATEGY

2.5.1 Evaluation objectives

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

2.5.2 Evaluation metrics

As in previous years, the Agency developed an evaluation strategy and a set of evaluation metrics for 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 separated per activity type, given that different information is relevant depending on the type of awareness campaign.

2.6 Campaign coordinators

Table 1: List of ECSM campaign coordinators for 2020

NATIONAL CAMPAIGN COORDINATORS					
Country code	**Country**	**Website**	**Country code**	**Country**	**Website**
AT	Austria	https://www.bka.gv.at/	IS	Iceland	https://www.srn.is/
BE	Belgium	http://www.ccb.belgium.be/en	IT	Italy	http://www.isticom.it/
BG	Bulgaria	https://e-gov.bg/	LT	Lithuania	https://www.nksc.lt/
CH	Switzerland	https://ibarry.ch/	LU	Luxembourg	https://cybersecurityweek.lu/
CZ	Czech Republic	http://ecsm.cz/	LV	Latvia	http://www.mod.gov.lv/
DE	Germany	http://www.bsi.bund.de/ecsm	MT	Malta	http://cybersecurity.gov.mt/
DK	Denmark	https://sikkerdigital.dk/	NL	Netherlands	https://alertonline.nl/
EE	Estonia	https://www.ria.ee/cert	NO	Norway	https://sikkert.no/
EL	Greece	https://saferinternet4kids.gr/	PL	Poland	https://bezpiecznymiesiac.pl/
ES	Spain	http://www.dsn.gob.es/	PT	Portugal	https://www.cncs.gov.pt/
FI	Finland	https://www.traficom.fi/	RO	Romania	https://cert.ro/
FR	France	http://www.ssi.gouv.fr/	SE	Sweden	http://www.msb.se/
HR	Croatia	https://www.cert.hr/	SI	Slovenia	https://www.varninainternetu.si/
HU	Hungary	https://kiberhonap.hu/	SK	Slovakia	https://www.sk-cert.sk/
IE	Ireland	https://dccae.gov.ie/			

3. EXECUTION PHASE

The execution phase of the ECSM campaign takes place during the month of October. During this period, EU Member States combine their efforts to raise cybersecurity awareness across Europe.

This year's campaign focused on the promotion of two themes: cyber scams and digital skills. The former was debuted at the beginning of the month along with the release of an accompanying awareness-raising video, with the campaign focusing on the second theme for the remaining 2 weeks of the month.

Efforts by the Member States were coordinated in 2020 via a 'content calendar'. The content calendar was developed jointly by the Agency and the contracted digital media company and was used as a guide for all Member States to collectively unite their promotional efforts for releasing ECSM material on specific targeted dates during October.

In parallel to the ECSM, Member States organised and executed their national campaigns with their own corresponding awareness material. An overview of 18 Member States and EFTA (16 MS and 2 EFTA) country campaigns and their corresponding activities is provided in Annex B of this report.

3.1 CAMPAIGN LAUNCH

The majority of Member States decided that the campaign launch should take place on 30 September rather than on 1 October with the launch of the press release. On 28 September, a teaser 'coming soon' video was released and on 30 September the press release was released along with the launch video by ENISA's Executive Director and DG Connect's Executive Directors.

The rest of the month was organised as planned and outlined in the content calendar.

3.2 CONTENT CALENDAR

The ECSM online campaign was planned and coordinated using a content calendar. The content calendar was distributed to all Member State coordinators and was validated in the monthly conference calls before execution. The content calendar included the release date of the material, a link to the material, a copy of the text to be used on social media platforms alongside the material when posting, and dates that the translated material would reach the Member States. This was to ensure that material was not released before a designated date and to amplify the results by acting in unison.

3.3 THEMES OF THE MONTH

'Think Before U Click' was the official motto of ECSM 2020. For the entire month of October, the programme focused on two themes to help people identify and be prepared for cyber threats.

The first theme, digital skills, provided participants with information on e-privacy matters such as personal data protection, cyberbullying and cyberstalking. The second theme, cyber scams, shared insights into current and potential cyber threats such as phishing, business email compromise and online shopping fraud.

ENISA and its partners published content and organised events and activities such as training sessions, strategy summits, presentations and more.

3.3.1 Weeks 1 and 2: 1–16 October – Cyber scams

The first theme, cyber scams, provided insights on current and potential cyber threats to help the general public and businesses minimise risks. COVID-19 has led to an increase in e-commerce, which has triggered concerns about the security of data and online payments. Activities in this theme focused on phishing, business email compromise and online shopping fraud. The key message encouraged users to have a heightened awareness of cyber scams when conducting business and personal transactions online.

3.3.2 Weeks 3 and 4: 17–31 October – Digital skills

The second theme, digital skills, presented educational activities for the public on internet security. The COVID-19 pandemic has increased the digitalisation of everyday life. This new hyper-connected world requires citizens to have an awareness of current skills to stay on top of trends and be safe online. The theme covered e-privacy matters such as personal data protection, cyberbullying and cyberstalking. The key message conveyed the importance of cyber hygiene and establishing good practices online.

3.4 DIGITAL MEDIA CAMPAIGN EXECUTION

The materials produced by the digital media contractor included videos, quizzes, infographics and a large number of GIFs, all produced from the original content. The materials were translated and made available to Member States via email on the publication due date as per the content calendar. The Member States were tasked with proofreading and disseminating the material. No editing of the material or replacing of English with translated text was necessary this year, as had been done in previous years, which saved significant time and reduced errors during the production.

The digital media contractor was tasked with posting the campaign material through paid and organic posts on Facebook and only paid posts on Twitter. The ENISA team took care of the organic posts and, on Twitter, the additional tweets and retweets of campaign-related messages (e.g. tweets related to events and Member State initiatives). The social media advertisements were paid for by a different contractor. A EUR 10.000 budget was provided for this task and it was primarily used to amplify the reach and engagement of core material, such as the videos and infographics.

3.5 ECSM DIGITAL MARKETING STRATEGY AND SOCIAL MEDIA CAMPAIGN

The social media campaign was designed with different targets at different times throughout the month of October. The first week aimed to increase awareness and reach as many people as possible with maximum visibility. The second week aimed to encourage the people who saw ECSM posts and tweets to play and watch the ECSM video. The third week aimed to identify the people who watched the video and motivate them to seek out other digital media content. Finally, the fourth week aimed to encourage the audience to visit the ECSM website and learn more.

Figure 2: Planning of social media activities

On Facebook, the campaign initially targeted shoppers, educators, teenagers and people related to small businesses, public companies and the IT field living in EU Member States. The campaign went on to retarget those who engaged with the main video and/or short version of the main video and to target audiences similar to those people.

On Twitter, the campaign also targeted shoppers, educators, teenagers and people related to small businesses, public companies and the IT field living in Europe. For the advertisements that followed, the campaign retargeted the people who saw the main video and/or short version of the main video.

4. EVALUATION PHASE

This chapter documents the activities that occurred to evaluate the ECSM 2020 campaign. The evaluation activities comprised four parts, which are described in the next sections. First, Section 4.1 describes the results from the implementation of the evaluation methodology, with feedback provided by Member State coordinators. The results are presented in comparison with the equivalent results from 2017, 2018 and 2019. Second, Section 4.2 presents the Member State survey regarding the evaluation of the planning and execution of the ECSM. Third, Section 4.3 presents the web analytics, including results from the activities related to the ECSM website. Finally, Section 4.4 presents the social media analytics, including results from social media activities and the reach of the target audience.

4.1 ASSESSMENT OF IMPLEMENTED ACTIONS BASED ON THE EVALUATION METHODOLOGY

The evaluation metrics are a useful tool for collecting consistent information from Member State coordinators regarding the activities that they implemented during the ECSM. Given the different natures of the various ECSM activities, the evaluation methodology defined different metrics for each type of activity. The following categories of activities were identified, with each having its own metrics:

- conference/workshop activities,
- TV/radio advertisement activities,
- ECSM website traffic,
- social media activities,
- fair stand/exhibition and roadshow activities,
- merchandising, posters and leaflets,
- tests/quizzes,
- the ECSM organisation effort.

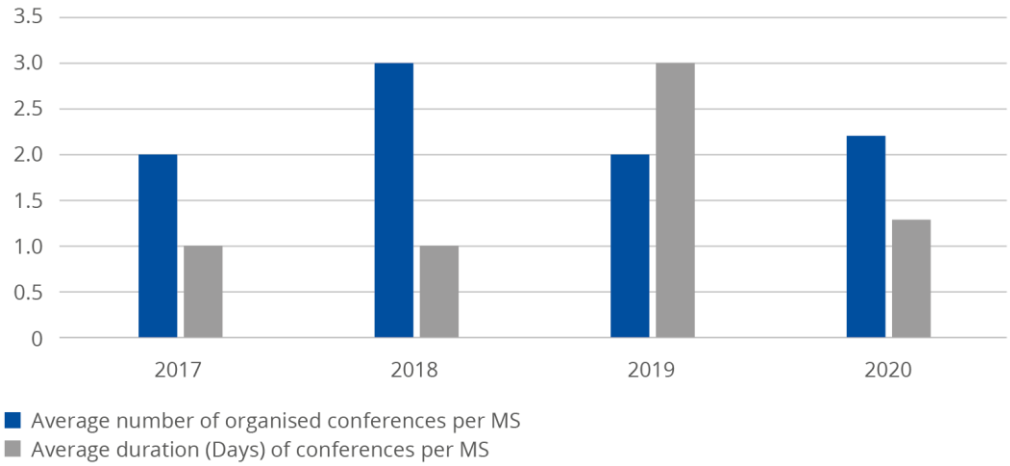
Table 2: Countries' annual participation in the evaluation

Country code	Country	2017	2018	2019	2020
AT	Austria				✓
BE	Belgium		✓	✓	✓
BG	Bulgaria		✓	✓	✓
CY	Cyprus				✓
CZ	Czech Republic	✓			✓
DE	Germany	✓	✓	✓	✓
EE	Estonia		✓		
EL	Greece			✓	✓
FI	Finland		✓	✓	✓
FR	France			✓	✓

Country code	Country	2017	2018	2019	2020
HR	Croatia				✓
HU	Hungary		✓	✓	
IE	Ireland				✓
IT	Italy				✓
LT	Lithuania				✓
LU	Luxembourg	✓	✓	✓	✓
LV	Latvia	✓			
MT	Malta		✓	✓	✓
NO	Norway	✓			
PL	Poland	✓		✓	✓
PT	Portugal		✓	✓	✓
RO	Romania		✓	✓	✓
SE	Sweden			✓	
SI	Slovenia			✓	✓
Total		**6**	**10**	**14**	**19**

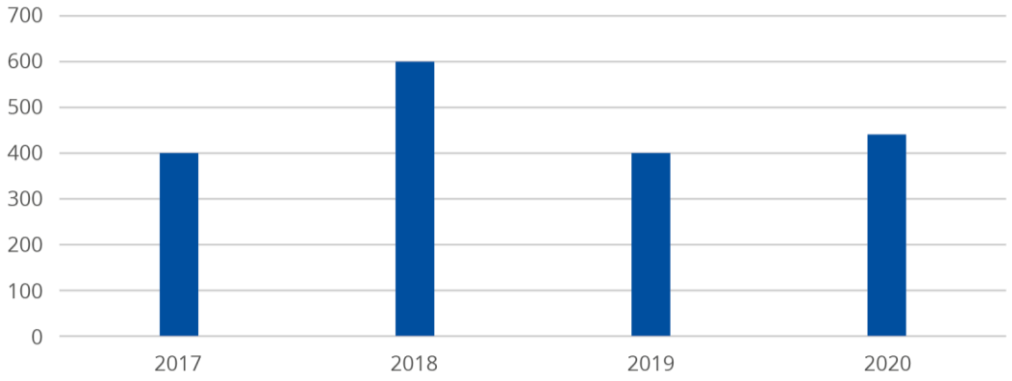
4.1.1 Results of conference/workshop activities

Figure 3: Average statistics of organised events across Member States and EFTA countries



According to the evaluation metrics survey, Member States reported that they had organised more events in 2020 than in 2019. The statistics refer to virtual events, as 2020 was the year of the COVID-19 pandemic. This may also explain the drop in duration in 2020, as most of the events took place virtually and within a shorter timeframe than events of the previous year.

Figure 4: Average number of attendees/participants at events across Member States

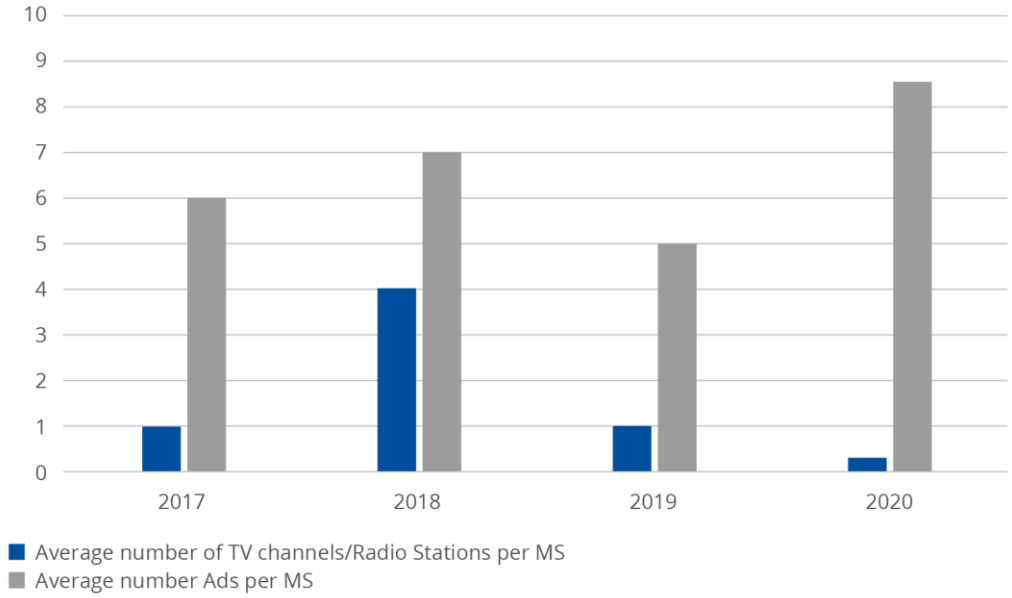


The number of participants in ECSM 2020 was significantly lower than in the 2019 campaign, possibly due to the COVID-19 pandemic and the associated national restrictions.

Participants provided positive feedback and were very satisfied with the content and approach.

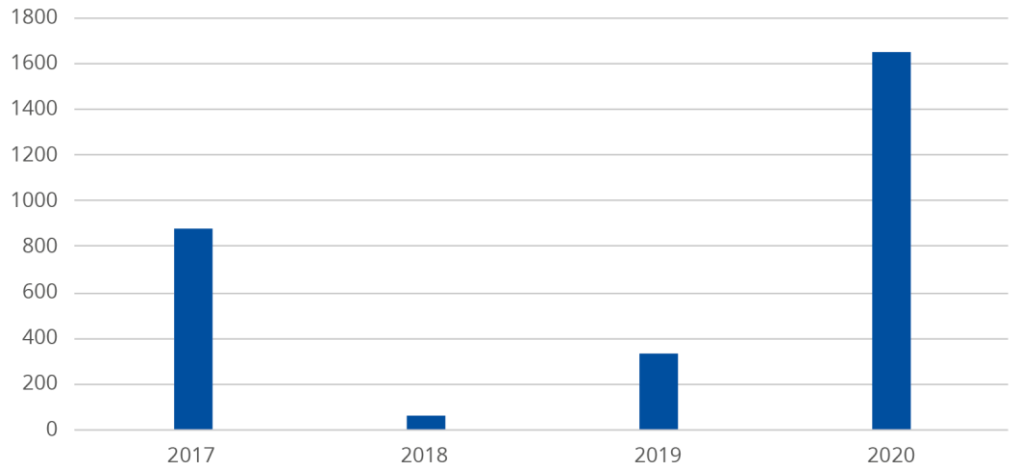
4.1.2 Results of TV/radio advertisement activities

Figure 5: Average number of TV channels/radio stations at which advertisements were placed and average number of times those advertisements were aired across Member States



Only 3 of the 20 participating countries placed TV or radio advertisements for ECSM 2020: Belgium, Bulgaria and Slovenia, and therefore the average across Member States was very low (represented by the blue bar for 2020). The average number of times these advertisements were aired (orange bar) was based on the data provided by these three countries.

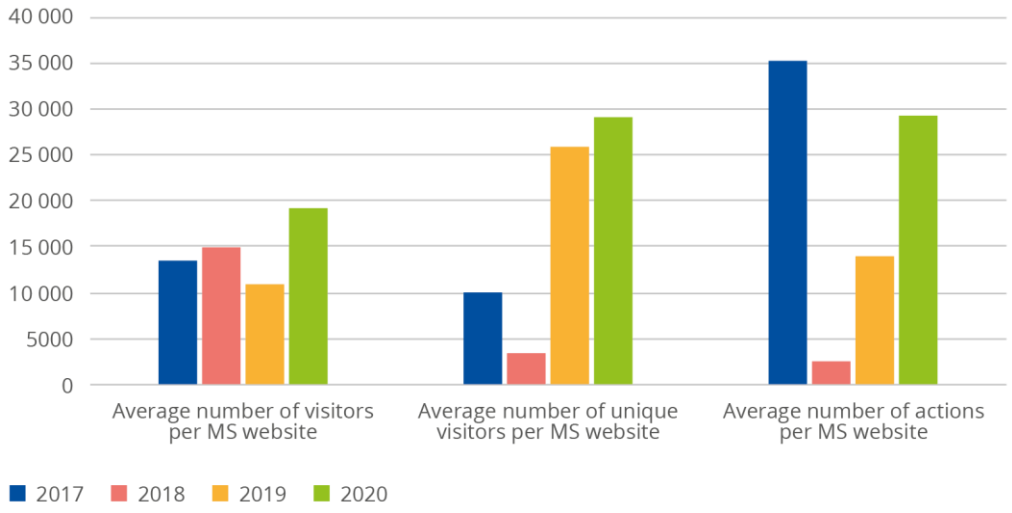
Figure 6: Average number of impressions across countries



The number of impressions corresponds to the average number of times that the ECSM advertisement was seen.

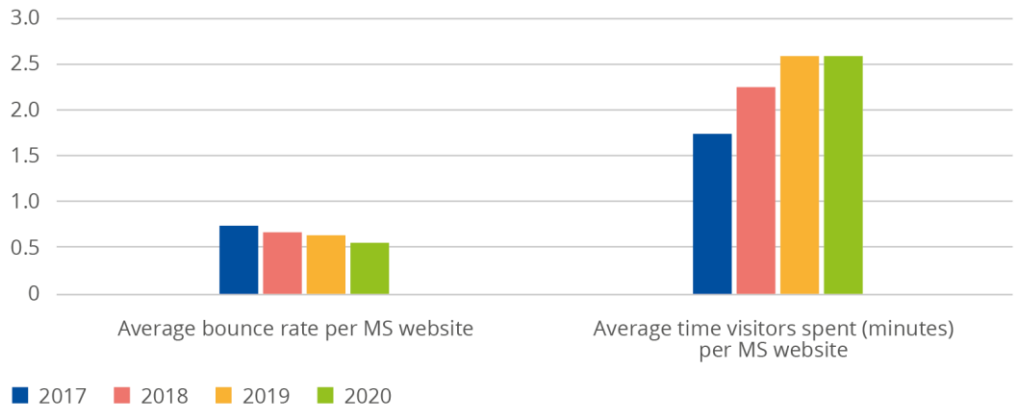
4.1.3 Results of Member States' website activities

Figure 7: Average number of visitors to and actions per user on Member States' websites



The average numbers of visitors and unique visitors increased in ECSM 2020 compared with the previous years. Similarly, the average number of actions per user was significantly greater in 2020 than in the previous year.

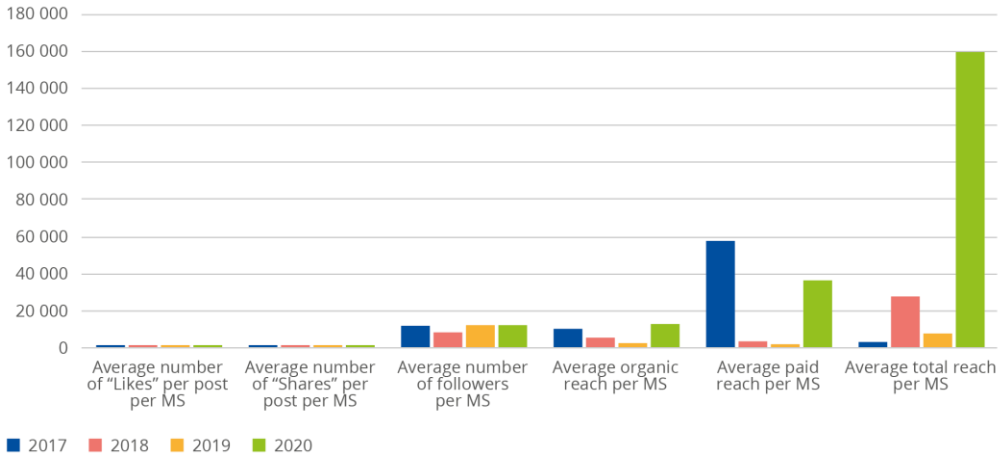
Figure 8: Average bounce rate of and time visitors spent on Member States' websites



The average bounce rate reached its smallest value in the ECSM 2020 campaign in comparison with previous years, while the time visitors spent on Member States' websites stabilised in 2020 and remained at the same level as in the 2019 ECSM campaign.

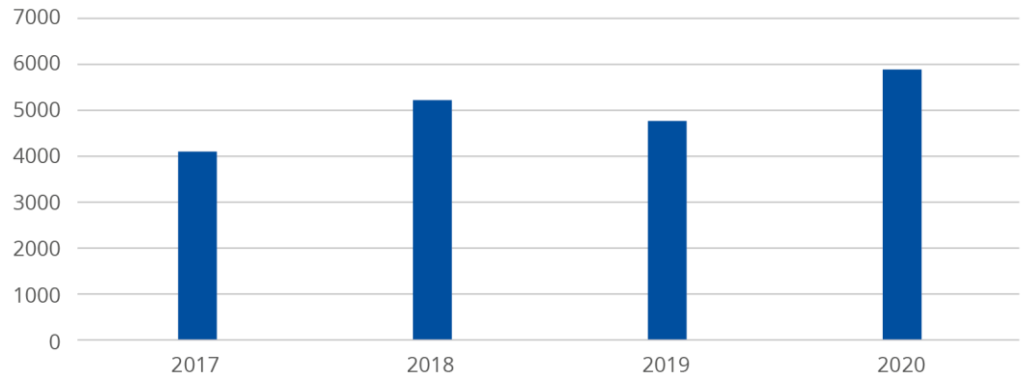
4.1.4 Results of social media activities

Figure 9: Average statistics of Facebook activities across Member States



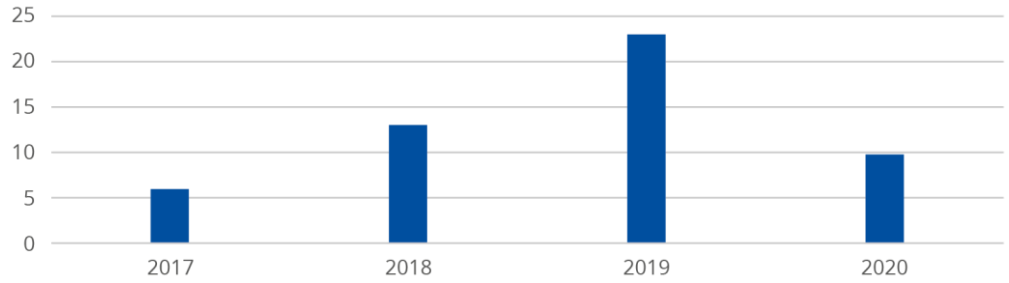
ECSM activities on Facebook are more popular than those on other social media. Figure 9 shows the activities that took place during October 2020 in relation to Member States' accounts and posts. On average, Member State coordinators increased paid Facebook activities and the number of followers, likes and shares in 2020, in comparison with 2018 and 2019. The number of followers slightly increased and the total reach substantially increased compared with all previous years.

Figure 10: Average number of Twitter followers across Member States



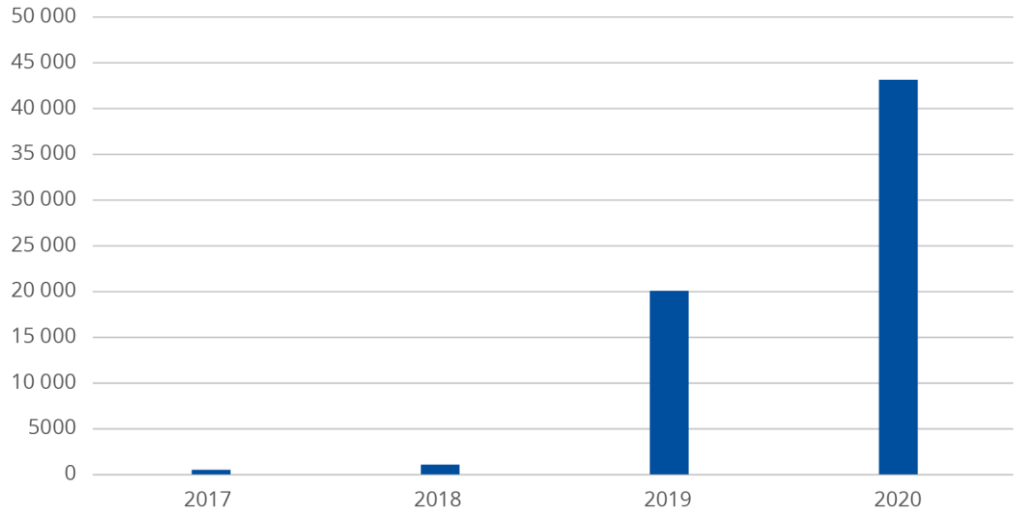
There was an increase in Twitter followers in the ECSM 2020 campaign compared with previous years, with an average of almost 6 000 followers across Member States.

Figure 11: Average number of retweets per post across Member States



Member States' Twitter activity was most effective in 2019, as the number of retweets was significantly higher than in all other years and was 2.5 times greater than in the ECSM 2020 campaign. In ECSM 2020, there were almost 10 retweets per post, on average.

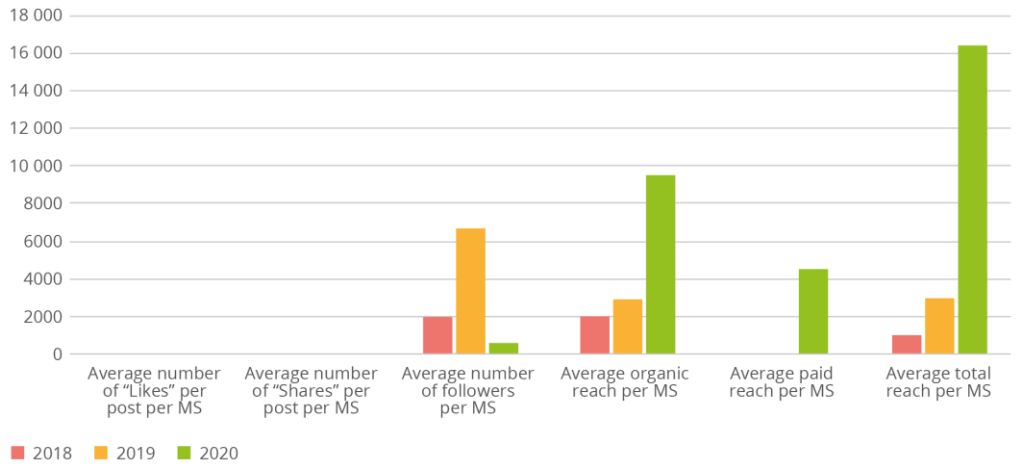
Figure 12: Average number of YouTube video views across Member States



YouTube video views reached the highest they had ever been during ECSM 2020, showing stable growth of the campaign's popularity throughout the years through YouTube. The statistics

were collected from six Members States (as opposed to eight in ECSM 2019); these were the only Member States that replied to this question of the survey.

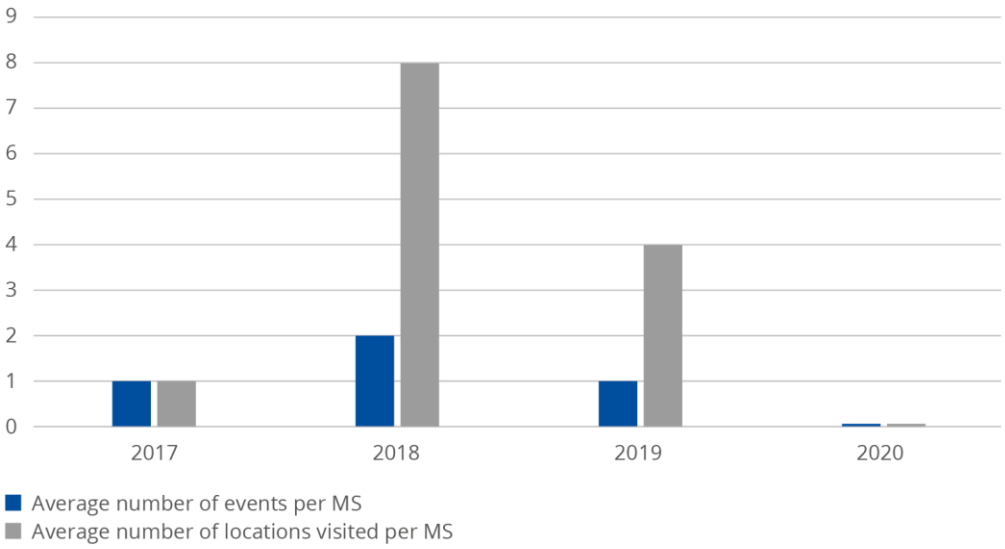
Figure 13: Average statistics of LinkedIn activities across Member States



These statistics do not represent the full number of countries participating in the campaign; only four Member States provided data (as opposed to five in ECSM 2019).

4.1.5 Results of fair stand/exhibition and roadshow activities

Figure 14: Average number of fair stand and roadshow events and locations visited across Member States



Owing to COVID-19, these events did not take place in 2020.

4.1.6 Results of merchandising, poster and leaflet activities

Figure 15: Average number of units and costs across Member States

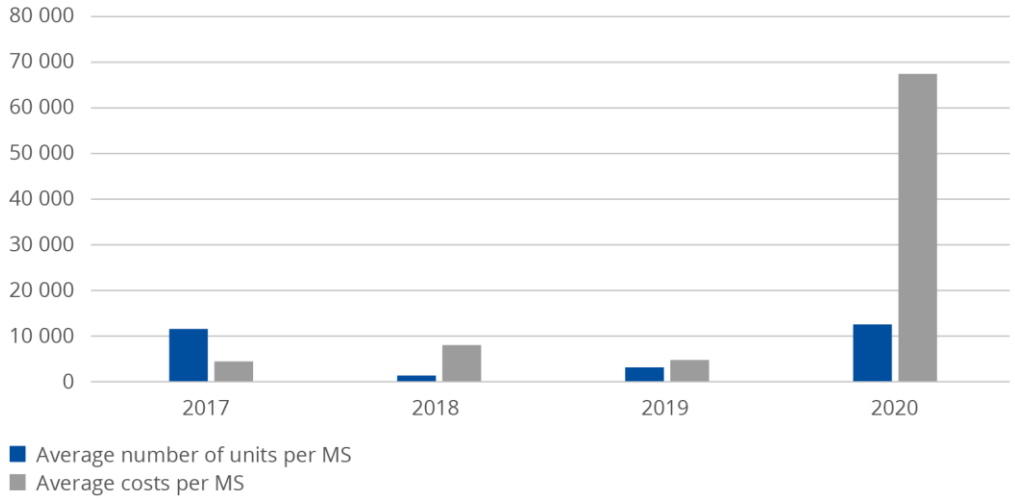
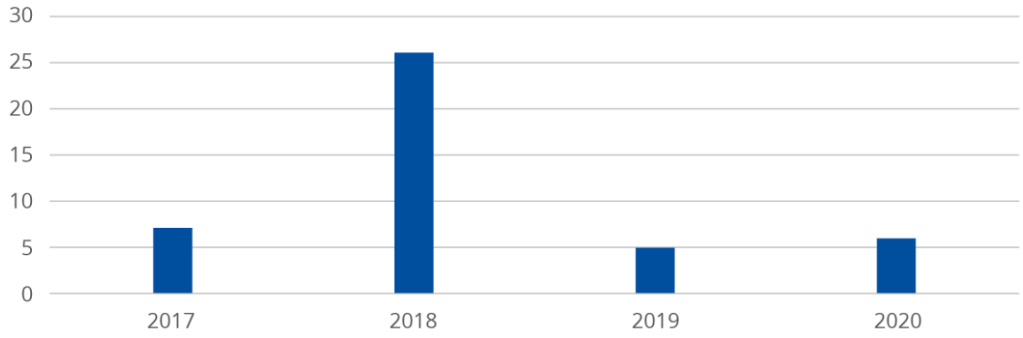


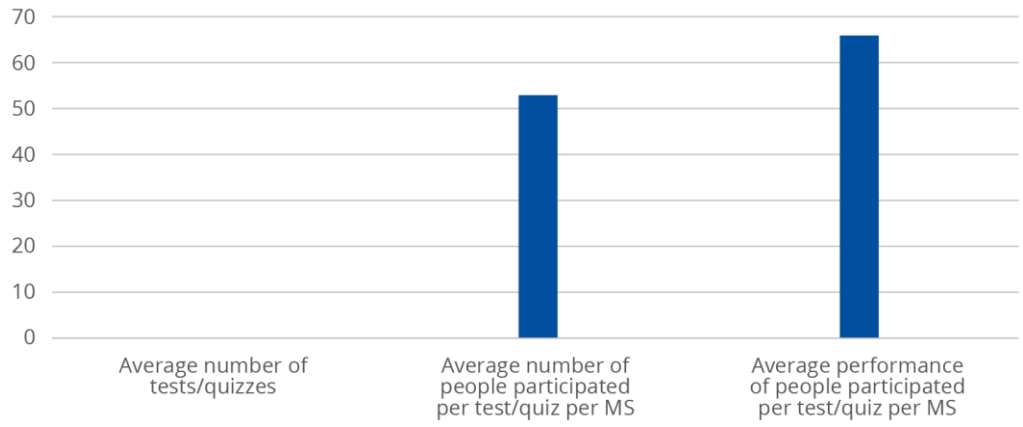
Figure 16: Average number of locations that awareness materials were distributed



4.1.7 Results of tests/quizzes

The implementation of tests/quizzes was not very frequent in 2020. Three countries implemented an equal number of quizzes and these were taken by a total of 160 individuals.

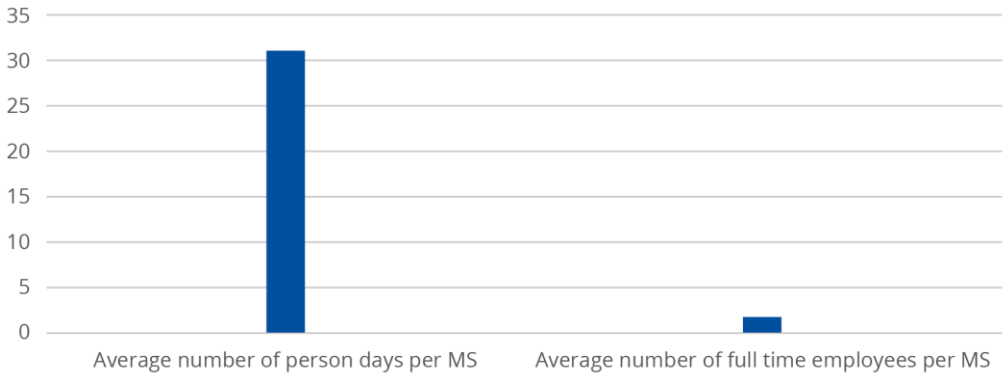
Figure 17: Average number of tests/quizzes, average number of participants and their average performance (%)



4.1.8 Results of the organisational effort

One or two full-time employees worked on average for each Member State for the preparation and execution of ECSM 2020, while 31 person days were allocated on average in each Member State organisation.

Figure 18: Average number of person days and full-time employees across Member States



The most prominent departments within each Member State organisation that engaged with the ECSM 2020 activities were the communications department followed by the information security and IT departments.

4.1.9 Consolidated results

This section reported on ENISA's continuous efforts to undertake a systematic and comparative analysis of the ECSM activities across Member States. In 2017, the Agency developed an evaluation strategy that was communicated to and agreed upon among Member State coordinators. The overall objective of this effort is to collect adequate information from the coordinators regarding the activities they organise during the ECSM each year and analyse them to produce useful findings for future ECSM organisations.

This section presented the comparative analysis of ECSM activities for 2017, 2018, 2019 and 2020, showing the average measures across participating Member States. The findings were divided per category of activity.

Regarding the organisation of conferences and workshops as part of ECSM 2020, the results showed a small increase in the number of events in 2020 in comparison with 2019; however, the duration of each event was significantly reduced, possibly because of the virtual organisation of many such events owing to COVID-19.

The number of radio and TV advertisements aired across Member States substantially increased in ECSM 2020. Similarly, access by visitors to Member States' websites increased in the ECSM 2020 campaign, with visits and actions per user increasing in comparison with previous years.

In the absence of physical events owing to COVID-19, great focus was given to promoting activities using social media, namely Facebook, Twitter, YouTube and LinkedIn, where all numbers showed an increase, with a significant increase in the total reach per channel of promotional activities.

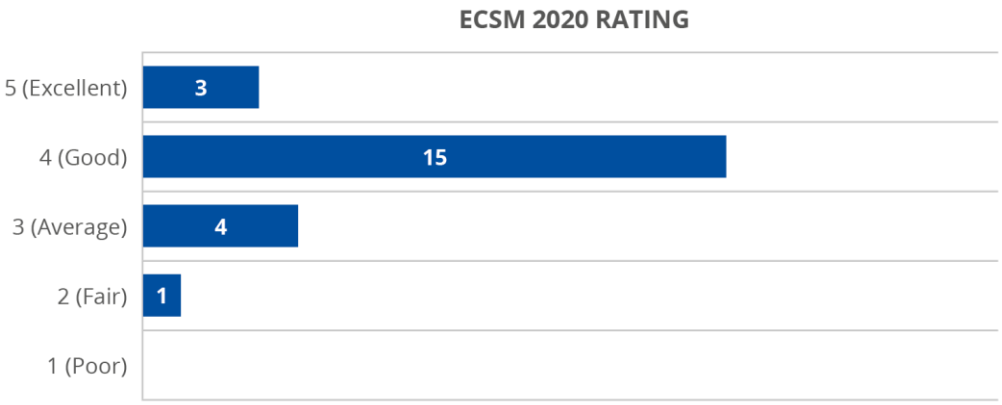
A general limitation as regards the findings of this evaluation is that the number of Member States that participate in the ECSM every year changes, making the results less comparable between years. However, this is expected to be remedied in future years.

4.2 ECSM CAMPAIGN SURVEY QUESTIONNAIRE

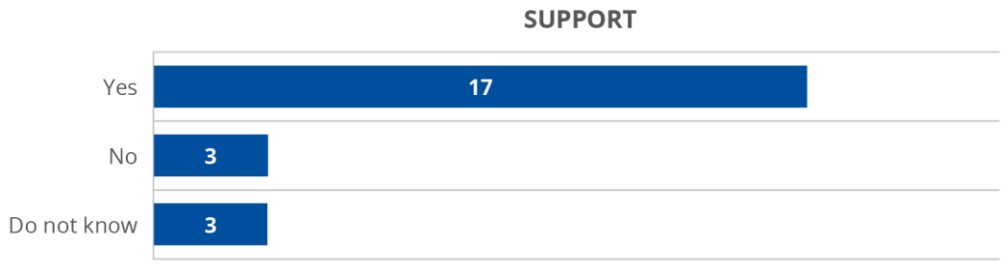
The questionnaire is an important tool that is used to gather the opinions of Member State coordinators engaged in the campaign. The charts in Section 4.2.1 present the anonymous replies of 23 participants representing their Member States. As shown in the consolidated results (Section 4.2.2), the ECSM is positively evaluated and is regarded as bringing additional value to Member States' national campaigns.

4.2.1 Member States' replies

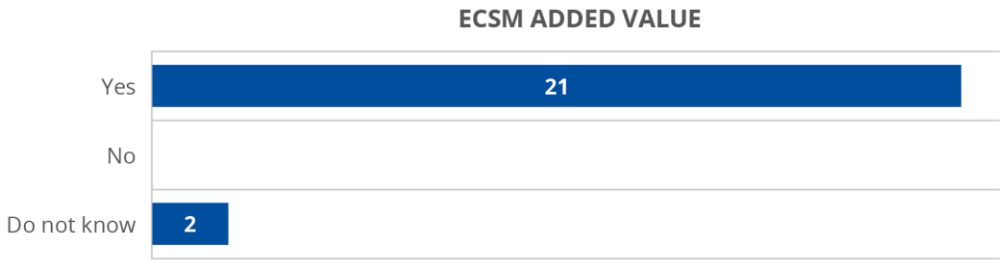
1. How would you rate the overall implementation of the ECSM 2020 campaign (scale 1–5)?



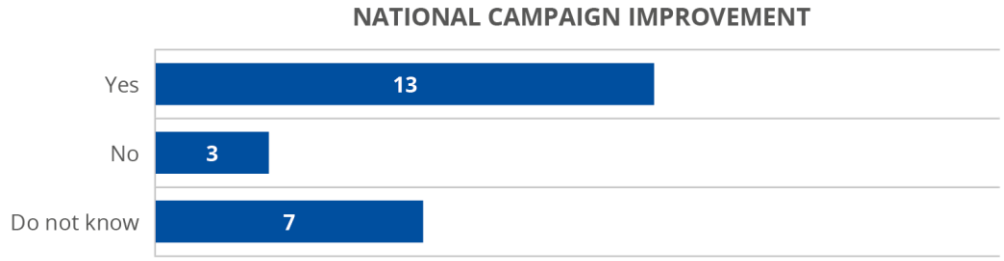
2. Did the ECSM support, in a satisfactory manner, the outreach and promotion of your work?



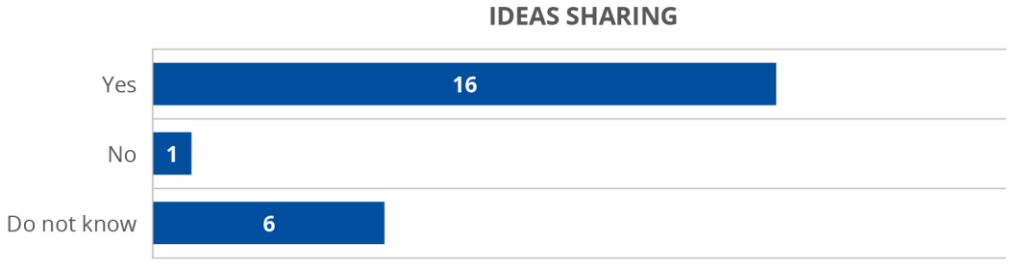
3. Did the ECSM add value to your national campaign?



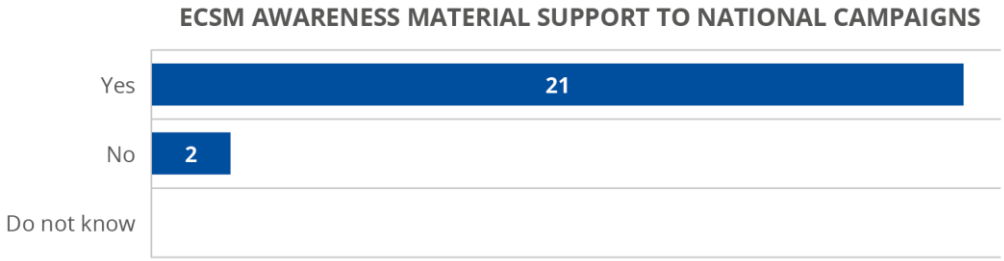
4. Did the ECSM offer opportunities for improving your national campaigns through collaboration with other countries?



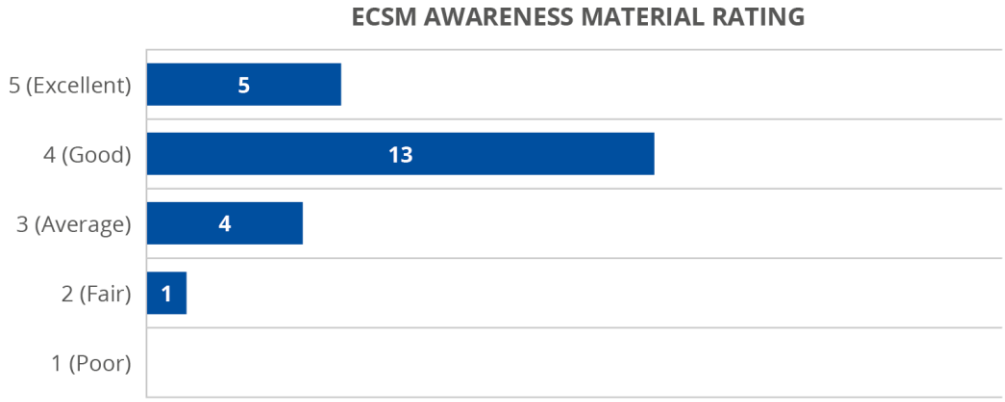
5. Do you think ENISA succeeded in sharing and promoting new ideas among ECSM partners?



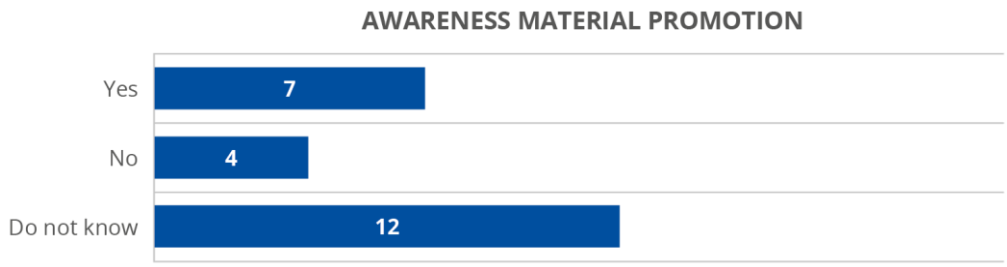
6. Did the material (videos, infographics, GIFs) produced by ENISA for the ECSM support your national campaign?



7. How would you rate the material produced for the ECSM 2020 campaign (scale 1–5)?

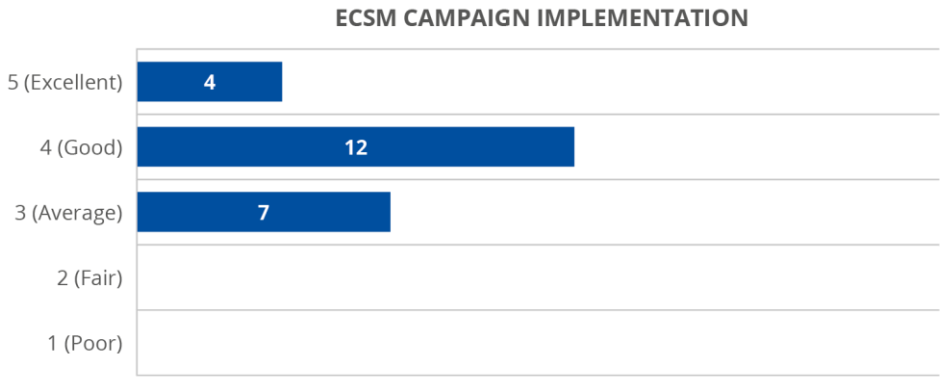


8. Could ENISA better promote your awareness material?



9. Do you think the ECSM offers opportunities for fostering a pan-European cybersecurity culture?

10. How would you rate the implementation of the ECSM 2020 campaign by ENISA (scale 1–5)?



4.2.2 Consolidated results

Most Member State coordinators (78.2%) rated the organisation of the ECSM campaign as good or excellent (question 1). Additional comments from Member State coordinators included a proposal for the earlier planning and delivery of ECSM awareness material to the Member States, allowing them time to prepare and to integrate them into their own campaign planning.

In 2020, the overwhelming majority of Member State coordinators agreed that the campaign supported and added value to their national campaign activities throughout the promotion of their work (questions 2 and 3). Some coordinators indicated that Member States should be more proactive with sharing information on their activities and two asked to receive the material at an earlier stage of the planning phase in order to better prepare and adapt official promotional materials (videos/infographics) provided by the Agency. In addition, in the context of question Q3, one coordinator suggested that during the ECSM all Member States should share with the Agency links to and materials for their activities, enabling the Agency to better promote the ECSM. The majority of Member State coordinators (57%) were convinced that the campaign offered opportunities for collaboration with other countries and for the improvement of national campaigns, while the remaining (43%) believed this was not the case or were uncertain (question 4). In addition, many Member State coordinators (69.5%) believed that the sharing

and promotion of ideas among coordinators was successful and beneficial to the national campaigns (question 5).

The feedback regarding the added value that this year's ECSM awareness material brought to the national campaigns proved to be very positive, as stated by the overwhelming majority (91%) of Member State coordinators (question 6). In addition, the majority of coordinators (78.2 %) rated this awareness material as good or excellent (question 7), with some suggesting that the awareness material should use a more modern design and animation.

The answers to question 8 were fairly split. Most Member States were uncertain about whether or not awareness material could be better promoted, while 7 of the 23 participating Member States suggested that there was room for improvement. The following suggestions were made on how better promotion of material could be achieved:

- better sharing of resources, which should be easy to implement via the website;
- increased shares and likes;
- sharing the material through the Agency's social media;
- making more efficient use of social media.

In response to question 9, the vast majority of Member State coordinators (87%) agreed that the ECSM offers opportunities for fostering a pan-European cybersecurity culture, while a significant proportion (69.5%) rated the implementation of the campaign as either good or excellent (question 10). Nevertheless, more than a quarter of the coordinators believe that there is space for further improvement, rating the implementation as average. One national campaign coordinator noted that 'visuals and resources should be made available earlier', emphasising the need for earlier preparation and provision of awareness material (graphics/videos) to the Member States for use in their campaigns.

Overall, the ECSM campaign received positive feedback in 2020. The overwhelming majority of coordinators gave the ECSM a good/excellent rating and believed that the campaign had supported, added value to and improved their national campaigns and had promoted the sharing of ideas between the Member States.

Moreover, the ECSM team received very positive feedback with respect to the provision of promotional and security awareness materials, especially in relation to the Member States having limited resources for such production.

Nevertheless, while on the one hand most coordinators gave the awareness material produced a very high rating, the majority still thought that the ECSM campaign could better promote Member States' activities and awareness material (i.e. among Member States but also to the public). In addition, coordinators also pointed out that a greater effort had been made in 2020 as regards Member State collaboration and organising joint activities, while also making a reference to this year's pandemic, which hindered the organisation of in-person events.

All coordinators agreed that for both 2019 and 2020, the ECSM campaign offered opportunities for fostering a pan-European cybersecurity culture.

4.3 WEB ANALYTICS

Web analytics provided the statistical data for the ECSM website and social media channels. The purpose of gathering these statistics was to evaluate the impact and visibility of the campaign.

4.3.1 ECSM website

The analysis took into consideration multiple variables in relation to different types of access points to the ECSM website for the month of October 2019 and included:

- page views – 117 072 (in comparison with 102 945 in 2019),
- website visits – 35 445 (in comparison with 30 807 in 2019).

Figure 19: Overview of ECSM website visits in September and October 2020

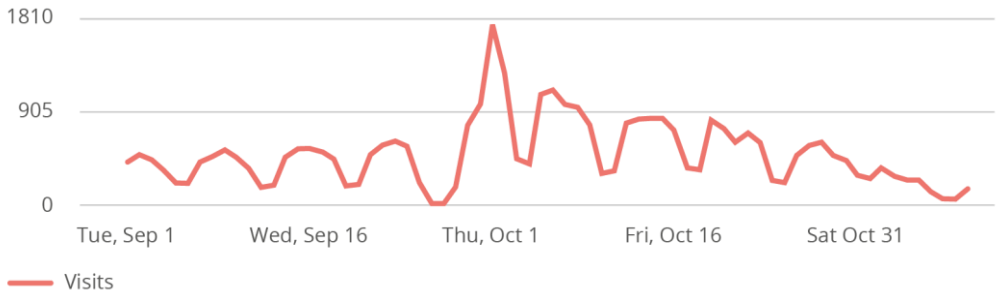
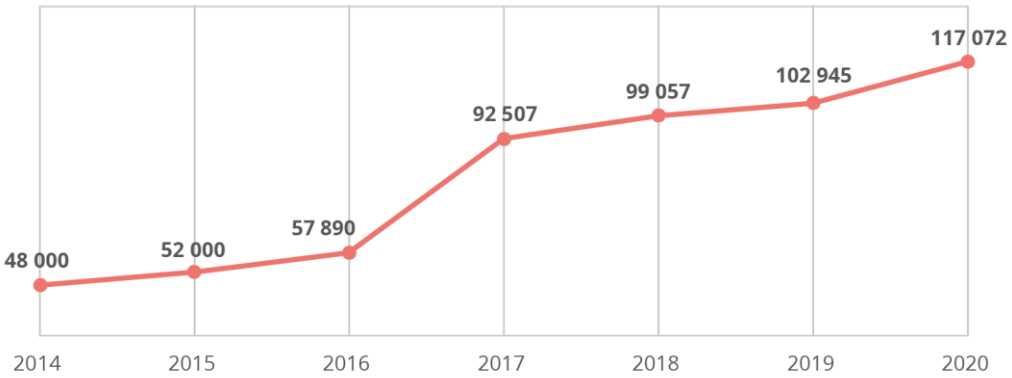


Figure 20 shows the number of page views that the ECSM website has had from 2014 to 2020. It demonstrates that visits to the ECSM website continued to grow in 2020, namely at a rate of 13.7 %, which is greater than the growth rate of any of the ECSM campaigns of previous years.

Figure 20: Page views of the ECSM website from 2014 to 2020



4.3.2 ECSM map of activities

Figure 21 illustrates the total number of events that have taken place in October (top graph) and the number of Member States, European Free Trade Association (EFTA) countries and other European countries that have organised at least one event/activity (bottom graph) from 2014 to 2020.

Figure 21: Number of activities in October (top) and number of countries registering activities (bottom) annually

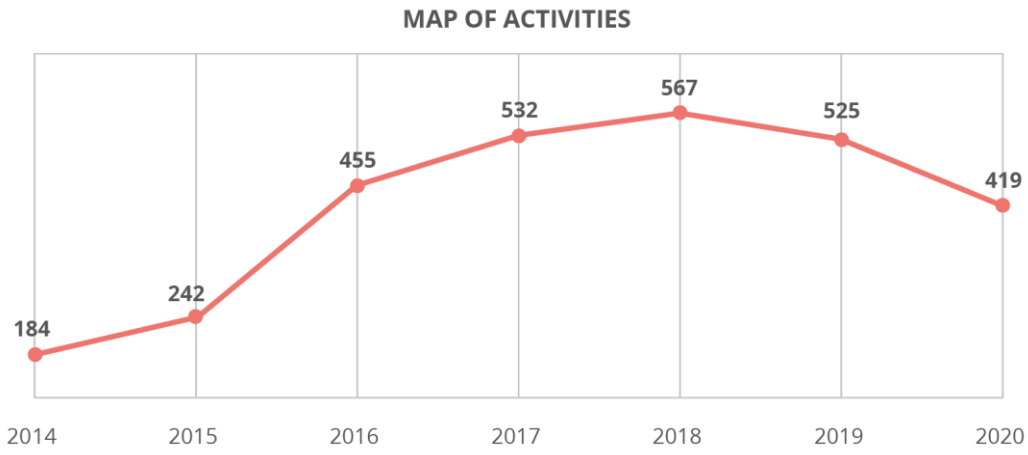
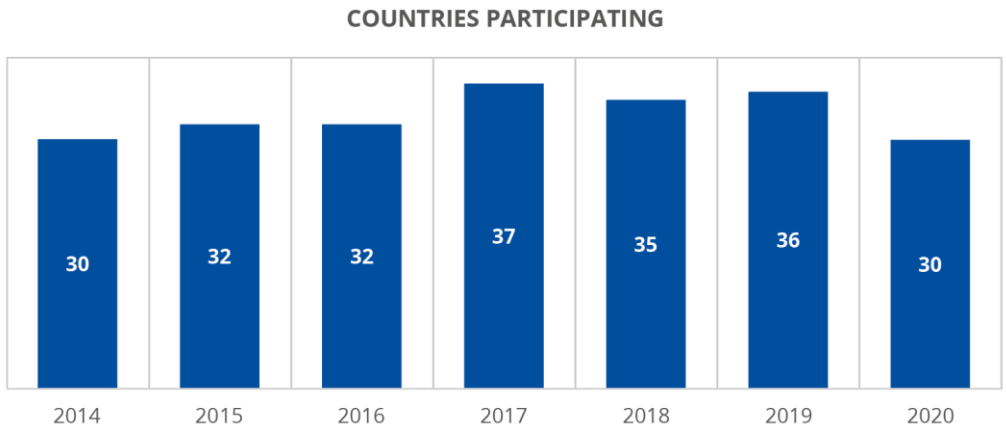


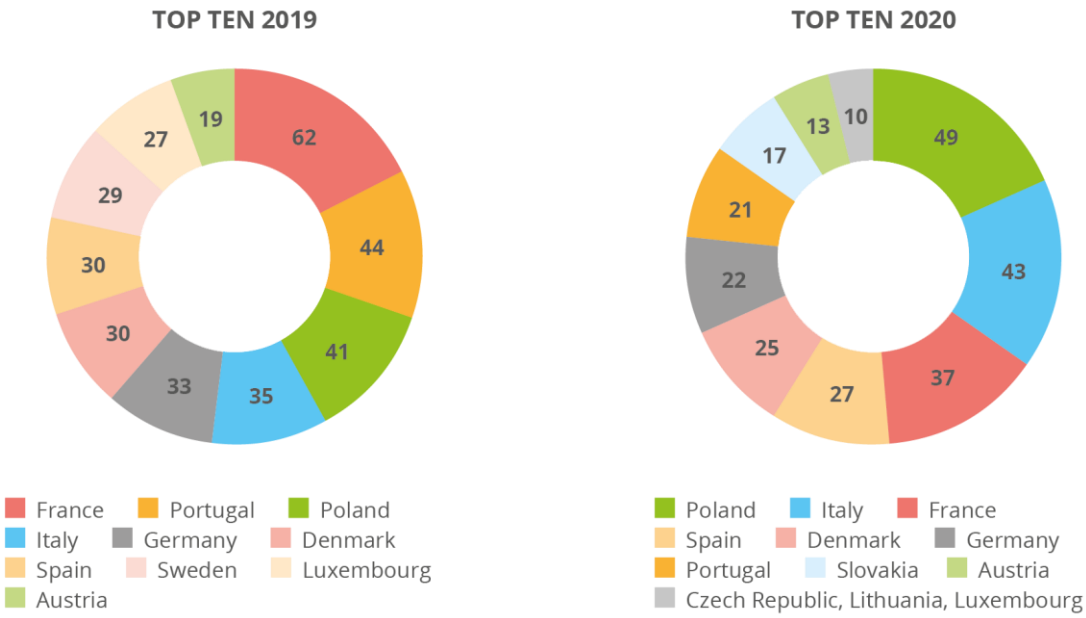
Figure 21: Number of countries registering activities annually



There was a decrease in 2020 in the registration of activities owing to the COVID-19 outbreak. In total across all Member States, there were 419 events registered in 2020.

The top 10 Member States with respect to the number of events registered during October in 2019 and 2020 are displayed in Figure 22. A notable difference from last year's campaign is that, in 2020, Poland was ranked in first position, with 49 registered events, and there were new appearances of Slovakia, Czechia and Lithuania in the top 10 – namely in positions 8 and 10, respectively. Poland, Italy, France, Spain, Denmark, Germany, Portugal, Austria and Luxembourg managed to maintain their presence in the top 10 countries with registered cybersecurity activities.

Figure 22: Top 10 Member States with respect to the number of events registered for ECSM 2019 and 2020



4.3.3 Social media analytics

Twitter continues to be a useful tool in the promotion and outreach of the ECSM campaign. Figure 23 demonstrates the fluctuation of Twitter followers for the handle @CyberSecMonth from September to November 2020. The highest peak corresponds with the launch of the ECSM, specifically the kick-off dates of the campaign around 1 October, followed by renewed interest until the end of the month.

The following are some useful statistics that were extracted from our web analytics:

- 1 562 new accounts were created within this period of 3 months;
- the total number of followers reached 24 681 (compared with 20 602 in the same period of 2019).

Figure 23: Daily growth of Twitter followers from September to November 2020

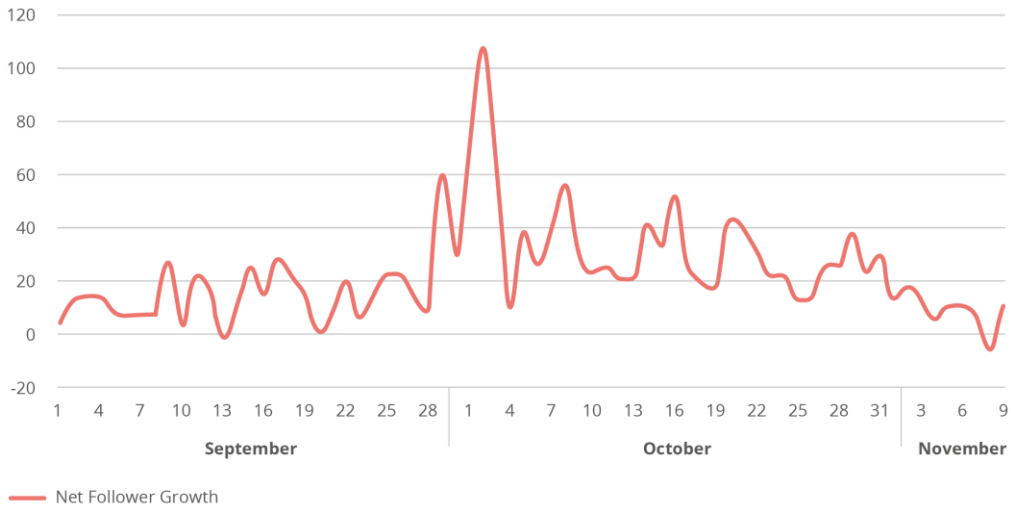
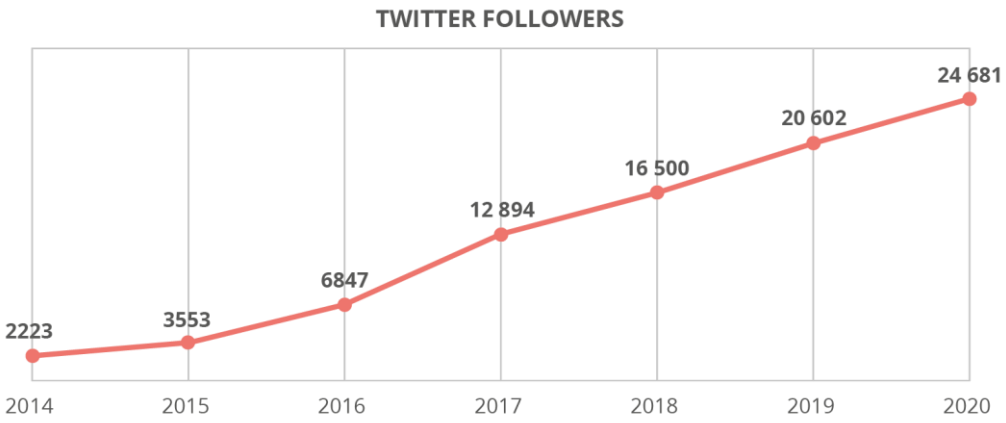


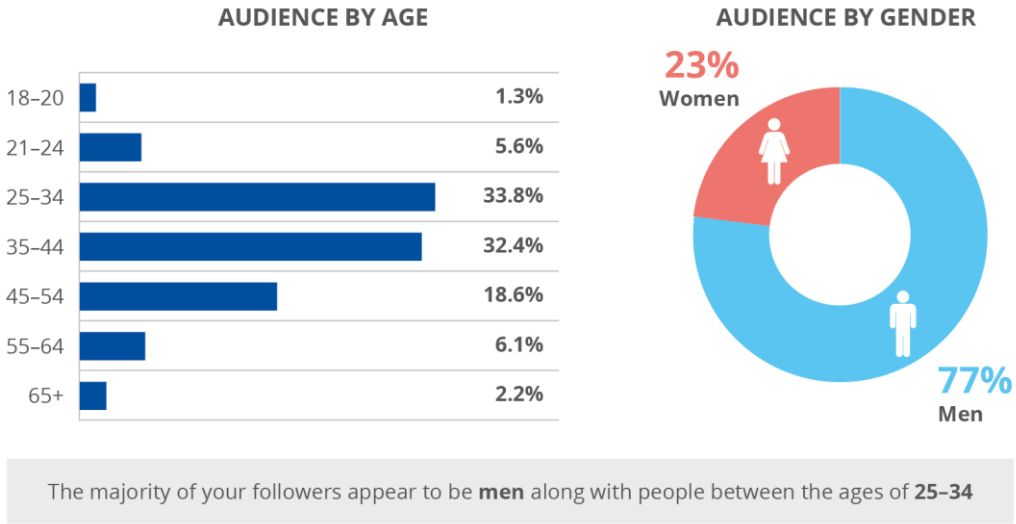
Figure 24 tracks the growth in Twitter followers of @CyberSecMonth from 2014 to 2020. It shows accelerated growth in this year's campaign, reaching a 20 % increase from the previous year.

Figure 24: Annual number of Twitter followers of @CyberSecMonth



Twitter demographics by age and gender identified the largest group of followers to be those aged 25–44 years of age, making up 66.2 % (compared with 64.3 % in ECSM 2019) of the total audience. Men were the leading force among followers (77 %), while 23 % were female (exactly the same as in ECSM 2019).

Figure 25: Twitter followers by age and gender



4.3.4 Social media reach

ECSM 2020 was supported by an impactful digital media cross-channel campaign led by the hashtag #CyberSecMonth. This year's campaign has been a particular success in comparison with previous years in terms of social media reach and other statistics, as the following statistics for the period from 1 September to 8 November indicate:

- social media reach – 9.8 million (compared with 2.7 million in ECSM 2019);
- mentions – 7 046 (compared with 1 928 in ECSM 2019);
- shares – 10 613 (compared with 3 727 in ECSM 2019).

The campaign's social media reach substantially increased in ECSM 2020 compared with 2019, namely by 148 % for social media reach, 265 % for mentions and 184 % for social media sharing.

Figure 26 provides an insight into the statistics of the #CyberSecMonth campaign and of the general exposure of the digital campaign supporting ECSM.

Figure 26: High-level statistics of ECSM 2020 for the #CyberSecMonth campaign

7046 MENTIONS	6734 SOCIAL MEDIA MENTIONS	312 NON-SOCIAL MENTIONS	8.8 M SOCIAL MEDIA REACH
511 K NON SOCIAL MEDIA REACH	30 677 INTERACTIONS	10 613 SHARES	20 064 LIKES
2104 100% POSITIVE MENTIONS	0 0% NEGATIVE MENTIONS	23 MENTIONS FROM BLOGS	6707 MENTIONS FROM TWITTER

Figure 27 gives an overview of the overall online reach for each of the ECSM campaigns since their kick-off in 2014.

Figure 27: Overview of the campaign's overall online reach from 2014 to 2020

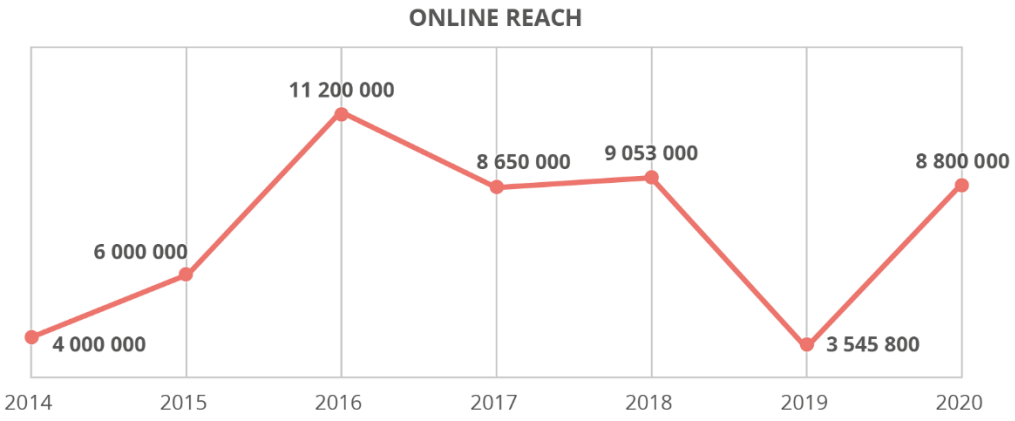


Table 3 shows the number of mentions and the reach of the top 20 countries in the context of the #CyberSecMonth campaign. These statistics are estimations based on the geolocation of IP addresses.

Table 3: Number of #CyberSecMonth campaign mentions per country on a worldwide scale

Most active countries

	COUNTRY	MENTIONS	REACH
1	Italy	281	246 475
2	United Kingdom	215	99 882
3	Norway	137	158 972
4	Spain	91	123 722
5	Romania	85	29 930
6	Greece	60	28 994
7	France	58	63 186
8	Germany	46	129 298
9	Belgium	39	110 723
10	Ireland	38	32 089
11	Iceland	37	32 380
12	Poland	35	2879
13	United States	30	114 174
14	Croatia	29	2724
15	India	28	279 826
16	Slovenia	27	13 397
17	Czech Republic	25	1071
18	Lithuania	21	5534
19	Mexico	20	18 839
20	Bosnia and Herzegovina	19	4032

4.3.5 Assessment of the ECSM digital marketing strategy and social media campaign

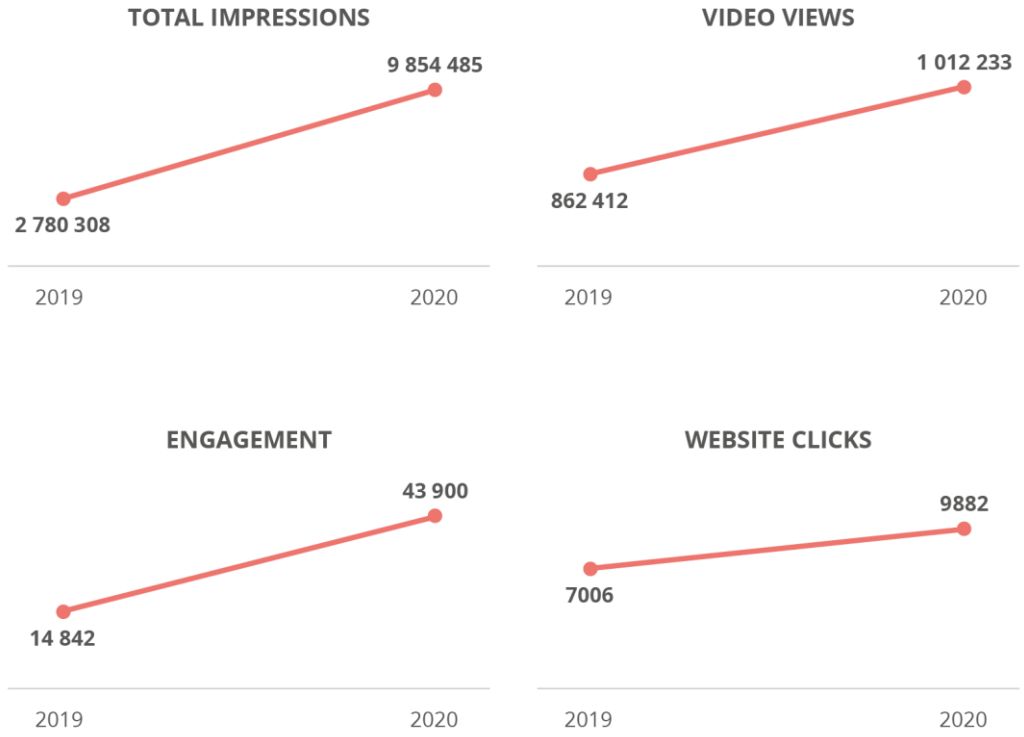
During the planning phase, the digital marketing analysts assessed the ECSM's existing digital channels, assets and content; this was followed by the development of new content for owned and earned media campaigns. Assessment metrics were specified to evaluate the effectiveness of the newly developed digital marketing and social media campaign. The results of this effectiveness assessment, measured from 1 September to 9 November, are presented in Table 4.

Table 4: Social media campaign effectiveness

Effectiveness metric	Communication channel	Results
Total impressions (of the material posted via ECSM channels)	**All**	**9 854 485**
	Facebook	4 994 850
	Twitter	5 185 999
Video views (multiple videos – aggregate performance)	**All**	**1 012 233**
	Facebook	971 500
	Twitter	40 733
Engagement (likes, clicks, shares, etc.)	**All**	**43 900**
	Facebook	22 666
	Twitter	27 637
Website clicks	**All**	**9 882**
	Facebook	8 487
	Twitter	1 395

This year was the second year in which the above social media campaign effectiveness metrics were recorded and they can therefore be compared only with last year's campaign (Figure 28).

Figure 28: Comparison between ECSM 2019 and 2020 for the social media campaign effectiveness metrics



4.3.6 Consolidated results

The majority of the indicators used to evaluate the campaign demonstrate a higher growth rate year on year. For this year, growth in the numbers for the ECSM website and social media channels has been noticeable.

ECSM page views have shown a steady increase since the kick-off of the ECSM in 2014, as a result of the continuous growth of the campaign and its popularity. Visits to the ECSM website in 2020 increased by 15% in comparison with 2019.

In support of this finding of increased growth and popularity, the social media reach recorded for ECSM 2020 reached 9.8 million, compared with 2.8 million in 2019, namely a threefold increase. Other numbers, such as mentions, posts sharing, website visits, video views and total impressions, all indicate a significant increase in comparison with 2019.

5. CONCLUSIONS

This official project deliverable outlines the main findings of the ECSM campaign in terms of the planning, execution and evaluation phases. The evidence collected has been synthesised to identify overarching patterns, the perceived quality and the campaign's success in achieving the goals and objectives specified. The evaluation of the campaign was based on the analytical data gathered, the feedback received from the Member State questionnaires and the social media and website analytics.

5.1 PLANNING PHASE

The in-person meetings organised by the Agency during the planning phase was integral for effective planning and especially for deciding with Member State coordinators the themes of the ECSM, the collaboration infrastructure and the organisation of activities for the ECSM.

A key element resulting from the planning phase were the cybersecurity themes that the ECSM monthly activities would promote to the target audience. All previous campaigns were organised around four themes, one per week, until 2019. ECSM 2020 included two main themes instead of four to provide more content and focus, as was done in the previous year (2019). Another key decision of the planning stage was the enrolment of a digital media company by ENISA to assist in the design of material and messages for a digital media strategy, including the development of material and an assessment of social effectiveness. Finally, during the planning phase, it was decided that two task forces would be put together for message content creation and target audience specifications around the two campaign themes.

5.2 EXECUTION PHASE

The use of two themes instead of four allowed the Agency and Member States to maintain a greater focus on certain areas of cybersecurity, thus allowing the conception, development and promotion of more clear and consistent messages throughout the campaign.

The campaign would certainly benefit from a governance structure and well-defined milestones throughout the whole year, not just in October. Such structure would help improve the organisation of task forces during the planning phase by having clear roles and responsibilities for each of the defined activities, thus overall help to improve coordination among Member States and the promotion of messages and awareness material.

The organisation of task forces – comprising representatives from Member States and the EU institutions who discuss and reach a consensus on the plan, target audiences and main messages of the ECSM campaign – should be repeated. The context and content of the messages and awareness material should be produced and published based on a timeline of release activities via the content calendar. The centralised model for translations proved to be more efficient than previous approaches and should be repeated.

The execution phase of the 2020 campaign was evaluated for each of its organisational aspects using the feedback and evaluation data metrics received from Member States, as presented below.

5.3 EVALUATION PHASE

Several of the factors that contributed to the success of the campaign in 2020 were:

- a 22 % increase in the number of Member States actively participating in the campaign compared with the previous years (an additional six Member States and one EFTA country) with the support of the National Liaison Officers (NLO) network;
- a fourfold increase in the production of campaign materials, especially videos;
- the launch of a new, more appealing, website for the campaign at which country coordinators could better showcase their work;
- outsourcing the design and creation of the marketing and digital media assets and doubling the budget spent on paid advertisements;
- targeting the media campaign to specific target audiences via specific media channels;
- the drafting of a campaign design, simple and compact messages, and calls to action by dedicated task forces made up of Member State coordinators, the European Commission and Europol;
- the translation and dissemination of all campaign materials centrally to Member States.

For the benefit of next year's campaign, the following outlines the key elements of success and the main challenges, leading to both strategic and practical recommendations.

This was the fourth year that evaluation metrics were collected from Member State coordinators, which allowed better insights to be gained for the assessment of the ECSM. The number of Member States contributing to the evaluation metrics has increased every year, from six in 2017 to 10 in 2018, 14 in 2019 and 18 in 2020. Although the results are averaged across Member States, not all Member States gave input on each of the metrics. More accurate and comparable results will be achieved only once all Member States provide comprehensive metrics year on year.

Workshop members acknowledged that there had been a substantial improvement in participatory planning processes and results in comparison with the experience from previous years. This was predominantly the result of input sent by participants before the workshop, which helped in gaining insights into planning and implementing an awareness campaign. The workshop helped to clarify the following aspects:

- the number of themes to focus on during the month;
- the needs of the target group;
- the best channels and ways to communicate and spread the message to the target group;
- the content of the message.

These aspects were further elaborated upon with the support of two task forces established by volunteers from the Member States, the European Commission and Europol.

The campaign was strategically focused to influence social media users to feel or act in a certain way. Facebook and Twitter advertising proved to be by far the most effective way to reach users, in terms of both reach and, more importantly, higher engagement rates. However, the use of LinkedIn was also improved this year by Member State coordinators. Social media campaigns are a lot more likely to get users to engage compared to other communication channels. Video advertisement campaigns are valuable marketing strategies that have a massive impact on the number of users visiting the ECSM website and engaging with campaign content.

The update of the ECSM website also proved to be a key factor in the campaign's success, as it contributed to the increased engagement and commitment by the Member State coordinators,

who were able for the first time to review and upload resources and events organised in their countries in a user friendly and secure way.

The evaluation of social media, media monitoring and website statistics consists of a multifaceted strategy to both investigate the immediate impacts of the project activities and create a baseline and follow-up opportunities for exploring longer term impacts. Undertaking future evaluation statistics also aligns with the recommendations from the workshop to seek external support for evaluating the success of the campaign.

In brief, we could draw the following conclusions:

- ECSM content became available to threefold more EU citizens in 2020 than in the previous years' campaigns (from 2.7 m to 9.8 m citizens);
- social media metrics showed an increase of traffic to all media channels, including the ECSM and Member State websites, Facebook, Twitter and LinkedIn;
- the number of participating Member States increased at the planning, execution and evaluation phases of the campaign compared with previous years, which was also an important factor in the success of the campaign in 2020.

5.4 RECOMMENDATIONS

The main recommendations deriving from the input received from the participating Member States are: a.to establish a governance structure to support the decision-making of the outreach programme and b. to maintain the campaign's engagement with EU citizens throughout the year (in addition to the campaign focus for the month of October).

ANNEX A: PRESS RELEASE

European Cybersecurity Month 2020 'Think Before U Click' kicks off today

This October marks the European Union's eighth European Cybersecurity Month (ECSM), promoting online security among EU citizens. The annual cybersecurity awareness campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission, and supported by the Member States and more than 300 partners from across industries.

Athens, 30 September 2020

Hundreds of activities, such as conferences, workshops, training sessions, general presentations, webinars and online campaigns, will take place across Europe for the entire month of October to raise awareness of cybersecurity and provide up-to-date digital security information through education and sharing of good practices. Each year, the European Cybersecurity Month brings together EU citizens to join forces under the slogan 'cybersecurity is a shared responsibility' to unite against cyber threats.

This year's ESCM campaign has been designed to address security issues surrounding the digitalisation of everyday life, accelerated by the COVID-19 pandemic. Encouraging people to 'Think Before U Click', the 2020 campaign highlights different cybersecurity themes to help users identify and prepare for cyber threats.

The first theme examines 'cyber scams' by sharing insights on current and potential cyber threats. Activities focus on phishing, business email compromise and online shopping fraud. The goal of this theme is to encourage users to have a heightened awareness of cyber scams when conducting business and personal transactions online.

The second theme centres around 'digital skills' by providing educational activities to inform the public on information security. The theme covers e-privacy matters such as personal data protection, cyberbullying and cyberstalking. The sessions aim to promote the importance of cyber hygiene and establishing good practices online.

Executive Vice-President for A Europe Fit for the Digital Age, Margrethe Vestager, said: 'As our daily lives and economies become increasingly dependent on digital solutions, we need to realise that cybersecurity concerns us all. It is important to foster a culture of state-of-the-art security across vital sectors of our economy and society.'

Vice-President for Promoting our European Way of Life, Margaritis Schinas, said: 'The European Cybersecurity Month aims at raising our cybersecurity awareness and getting us up to speed with the cyber threats; it reminds us that we can easily step up our own cybersecurity by getting into some good digital habits. Cybersecurity is essential for our European way of life.'

Commissioner for Internal Market, Thierry Breton, said: 'Just like land, sea or air space, the digital information space sometimes has security loopholes that need to be closed. Our ambition is to offer EU citizens the safest information space in the world. This will be achieved notably through education. This is what the European Cybersecurity Month 2020 is about, which we are launching tomorrow to boost awareness about online safety and the cybersecurity skills needed for the future.'

ENISA Executive Director, Juhan Lepassaar, said: 'This year's European Cybersecurity Month explores how to make our shared cyber ecosystem more resilient by sharing best practices and developing cyber skills. Being aware of cyber scams and thinking before you click are part of the easy-to-follow advice to limit risks. The ECSM allows us the opportunity to engage directly with EU citizens, businesses and organisations to raise their awareness of cyber threats, build on this knowledge and together advance cybersecurity on all fronts.'

Today, to launch the campaign, organisers published a video to provide EU citizens with tools to integrate into their daily cyber activities: https://youtu.be/G8kquD8cKYc

The official website of the ECSM campaign is https://cybersecuritymonth.eu/. Each participating EU Member State has a dedicated web page with updated information in the local language. Users can find tips and advice in 23 languages, awareness raising materials, online quizzes, links to events and more. The ECSM website also features a page where people can access and join activities.

Background

The European Cybersecurity Month (ECSM) is the EU's annual awareness-raising campaign dedicated to promoting cybersecurity, taking place each October across Europe. The ECSM is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission, and supported by the EU Member States and more than 300 partners (governments, universities, think tanks, NGOs, professional associations and private-sector businesses). The campaign first launched in 2012.

'Cybersecurity is a Shared Responsibility' – 'Think Before U Click'

Join the campaign on Twitter @CyberSecMonth with the hashtags #CyberSecMonth and #ThinkB4UClick, and on Facebook @CyberSecMonthEU.

Further European Cybersecurity Month information can be found at https://cybersecuritymonth.eu/.

###

For editors:

Cybersecurity Strategy of the European Union

ECSM Awareness and Educational Materials

ECSM: Get Cyber Skilled

Digital Single Market Strategy

Cybersecurity in the Digital Single Market

ENISA Guidance During COVID-19

European Cybersecurity Challenge

Press contact:

For questions related to the press and interviews, please contact press@enisa.europa.eu

ANNEX B: MEMBER STATE CAMPAIGNS OVERVIEW

This annex provides an overview of the campaigns executed at the Member State level, described in their own words.

BELGIUM

Passwords make us feel □□□□! Coming up with, remembering and using passwords is tedious, frustrating, time-consuming and not 100% secure either, as even the strongest password can be stolen and exploited. That is why the Centre for Cyber Security Belgium (CCB) is campaigning this year to promote better account security!

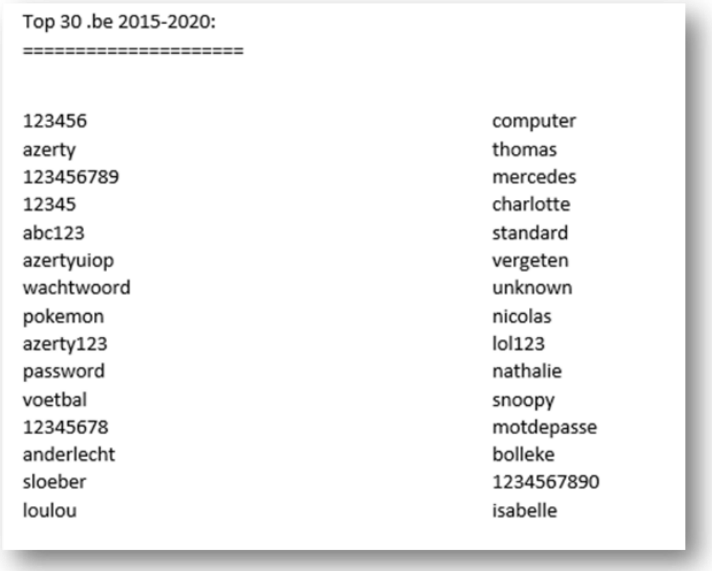
As part of the **European Cyber Security Month**, the Centre for Cyber Security Belgium (CCB) and the Cyber Security Coalition have launched a joint cyber security awareness campaign, for the sixth time. This year, we want to encourage internet users to apply stronger security measures for their accounts using **two-step verification**.

Online accounts (e.g. e-mail, social networks, online banking and online shops) are usually protected by a user name and a password. Unfortunately, users often choose passwords that are easy to remember and they also use the same password for different accounts. This makes it easy for hackers to gain access to those accounts. If an outsider gains access to an account, they can impersonate the owner and exploit it.

Forget about passwords!

The use of passwords is frustrating. You have to come up with new passwords all the time, they have to meet all sorts of requirements (special characters, upper and lower case, numbers) and they have to be long. So long that you invariably have to start over because of a typo. And so on and so forth.

Most Internet users are aware that a short and simple password is not good for them, yet we see that **weak passwords** are still used. 123456, qwerty, password, a first name, a favourite team, 'bolleke' or 'sloeber', these are just a few of the top 30 most frequently used passwords in Belgium. The shorter and simpler a password is, the faster it can be cracked even by novice hackers.



Frustrating, and also not entirely safe

Using strong passwords is an absolute must, but even then you still have to be careful. Strong passwords can also be stolen:

- Criminals try to steal your password by tricking you with a **phishing email**. They try to persuade you, for example, to enter your password in a fake website so that they can access your password.
- **Data breaches** are also frequent events. A platform you use, such as LinkedIn or Facebook may get hacked and all the users' data, including passwords, is stolen.

Sometimes we make life very easy for hackers:

- your passwords are on a Post-it hanging from your screen,
- you reveal your passwords on the phone, when you get a call from someone who pretends to be a Microsoft employee,
- you have entered your details to take part in some kind of competition,
- you store your passwords in a document on your computer called "passwords"

Using strong passwords is very important, but we recommend adding another layer of security: two-step verification (2FA).

Two-step verification (2FA): the solution!

Two-step verification or 2FA is a simple solution to better protect your accounts.

To access your account, you have to be able to prove that you are who you claim to be. There are three different ways, or factors, to do this:

- something only you know (your password or PIN number),
- something only you have access to (your phone or token),
- something that is a part of you (your fingerprint, face, iris, etc.).

Campaign material

We advertise on national and local television, radio, social media (Facebook and Instagram) and a free newspaper (Metro). More than 500 partners use our materials and share the campaign with employees, clients, students, etc…

View the campaign materials here.

Visit the campaign website.

Results

A survey conducted 2 weeks after the end of the campaign among a sample of 400 Belgians aged 16 and older showed that no less than 58% of respondents had noticed the campaign and 54% of those who had noticed the campaign had taken one or more actions. Our intention was to capture the attention of internet users and we clearly succeeded in doing so.

Many people look up information after they noticed the campaign, and talked about it with others. 14% of respondents said: 'I visited safeonweb.be'; 8% replied 'I looked up information about two-step verification'; 8% said 'I talked about it with friends, colleagues, family'; 8% responded 'I recommended two-step verification to friends, colleagues, family' and 7% said 'I looked up information about password managers'.

However, a lot of internet users took things a step further. 4% said "I enabled two-step authentication to log into at least 1 of my accounts", 4% replied "I helped someone set up two-step verification" and 10% said "I changed my passwords".

If we apply these figures to the entire population, at least 200,000 people have started using two-step verification. We owe these great results the many partners who campaigned together with us, such as Smartschool, the Belgian Federal Police and many cities and towns that shared the campaign through all their channels. Thanks to the Cyber Security Coalition, the campaign was picked up by numerous private, public and academic organizations, which is extremely important for its success.

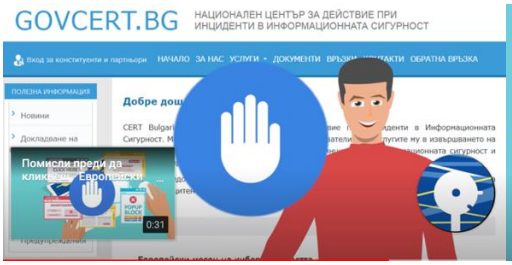
BULGARIA

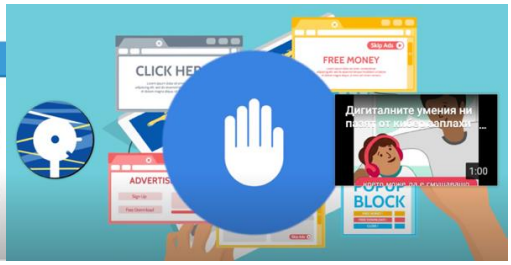
The kick-off activity for our campaign ‘Cyber Aware Week’, targeting children, parents and teachers, which was planned as a physical meeting, could not be launched as intended owing to the COVID-19 pandemic and the associated restrictions. Instead, the final week of October was dedicated to Facebook Live webinars that were very successful and reached more than 6 000 people over 1 700 engagements. In addition, two 30-second video teasers were shared over the course of 2 weeks (12–23 October) during prime time on national public TV to address the topics of digital skills and cyberscams.

In addition, a partnership was established with the three national telecommunications providers to send an SMS or a push notification to their users. The message was as follows: ‘Do you know what hides behind the link? Think before you click! Be careful online and improve your cybersecurity in the European Cybersecurity Month. More information on www.govcert.bg’. It reached more than 1.5 million service subscribers. One of the telecommunications providers sent a smart advertisement with videos to thousands of unique users, in addition to placing a banner on its mobile app to introduce the Facebook Live webinars.

Finally, a hybrid conference on the topic of cyber scams was co-organised on 7–9 October, featuring hands-on cybersecurity improvement workshops. A few interviews were conducted

that were published in a magazine and aired on the national public TV channel and on a local radio station.





CROATIA

The Croatian National CERT had several activities during the European Cyber Security Month that aimed at raising awareness of Croatian citizens about cybersecurity, with an emphasis on network and information security and promoting safer use of the Internet.

The following topics were covered:

- digital skills
- cyber hygiene
- digital trace
- Internet scam
- safe work from home.

Some highlights from the Croatian campaign involve:

- "Hacknite" - a competition for high school students https://www.cert.hr/hacknitenovosti

It was a competition for high school teams in the form of CTF (Capture the Flag) that raises awareness of the importance of applying security measures and avoiding and correcting possible security vulnerabilities in program code, settings or any other component of the computer system.

- "Countdown"

Interesting facts from the field of cyber security were published on the social media @CERT.hr and @HRCERT from the 15th of September to the beginning of October.
The Croatian National CERT also published a number of infographics on following topics:

- Digital trace (https://www.cert.hr/DIGTrag-InfoG)
- Cyber hygiene
- Internet scams
- Safe work from home (https://www.cert.hr/ROKCERT)

The campaign was advertised through the social media @CERT.hr and @HRCERT

CYPRUS

Our team made its first debut in the ECSM in 2020. Our strategy focused on closely following up with the ECSM social media, planned events and awareness material preparation by publishing, retweeting and reposting this material.

The main goal was to be active on social media. The fact that material was made by ENISA in both English and Greek allowed us to post in a timely manner in accordance with ENISA's schedule.

Examples of Twitter posts (https://twitter.com/NationalCsirtCy) are shown below.

Full articles following up on the tweets were reposted simultaneously on our website: www.csirt.cy

Our participation in the ECSM campaign offered us useful experience and the opportunity to learn valuable lessons, as we quickly realised that awareness material has a great impact on the social following of our organisation. Our plans for next year are to set a goal to prepare material and events tailored to our constituency.

CZECHIA

Our campaign's organisation targeted five main sets of activities on cybersecurity awareness and the dissemination of key messages to the public.

The first activity focused on the general cybersecurity awareness campaign and mainly included the dissemination of awareness materials prepared by ENISA, the Europol European Cybercrime Centre and the professional community. This campaign was launched in April 2020 and focused on both challenges related to COVID-19 (working from home, etc.) and topics promoted by the ECSM. The campaign took place virtually using social media (especially Twitter, Instagram, Facebook and LinkedIn), with some physical activities organised (e.g. advertising in public places).

Our campaign also aimed at raising cybersecurity awareness among students aged 9–25 years, an activity that was primarily implemented through the National Competition in Cyber Security (which reached out to approximately 50 000 students, with 4 000 students actively involved). Activities in this area are expected to continue until June 2021.

Additional professional and educational activities for secondary school teachers and for the professional community were also held. The activities for the former were implemented mainly through e-meetings and webinars. Teachers from 30 secondary schools throughout the country took part in these activities. The activities for the latter were targeted at representatives of the state and public administration, the critical information infrastructure and industry. Most of these activities were implemented with the support of partners from the public, academic and private spheres. More than 400 people actively participated in these activities and more than 1 000 people saw the recording of the e-activities.

Finally, we organised a cybersecurity festival, where a series of 10 online conferences and educational events were held focused on cybersecurity. This activity involved many partners and targeted various groups, such as teachers, parents and employees of non-profit organisations and public institutions.

DENMARK

ECSM 2020 was the second year that Denmark had the opportunity to participate in the ECSM. The Danish governmental Agency for Digitisation took over the role as national campaign manager. Based on the previous experience gained in ECSM 2019, we had already set the foundations for successfully advancing the cybersecurity awareness agenda in Denmark. Despite the unfortunate COVID-19 situation, we managed to bring together a broad range of collaborating actors and partners, namely national, regional and local public authorities, private companies, NGOs and influencers to contribute to the national discourse on cyber- and information security. They played a key role in sharing knowledge by participating in meetings, conferences, webinars and lectures, thus attracting interest from a variety of sectors in Denmark.

'One click may change everything' was the key message aimed at the general public in our national campaign this October. The target audience was primarily parents, and their main concerns were how to deal with the digital traps and pitfalls that their children may be exposed to. By taking a behavioural approach, we provided content on our website to support engagement in that specific area of concern. Thus, children and their parents were encouraged to participate in games, quizzes and tests on what to look for when using social media, shopping for goods and trading in online gaming.

The deeper message of 'One click may change everything' was to think before acting (and of course 'clicking') and was delivered in perfect alignment under the umbrella of the ECSM 2020 campaign.

In June, we began promoting our national cybersecurity month of 2020 on our permanent governmental website regarding information and cybersecurity, https://sikkerdigital.dk/. Since 2019, https://sikkerdigital.dk/national-cybersikkerhedsmaaned/ has been the national hub for all activities regarding the national cybersecurity month. In addition, in June, newsletters and direct mail were sent to the national agency's key stakeholders on cybersecurity inviting them to participate in the national cybersecurity month 2020.

Our website (https://sikkerdigital.dk/) is, along with our Facebook page (https://www.facebook.com/Sikkerdigital/), our main campaign and information channel aimed at the public, public authorities and SMEs.

Overall, the ECSM 2020 activities included:

- 30 registered campaign activities aiming at various target groups (public authorities, private enterprises, families, scholars, librarians, schools, etc.), conferences (webinars), online meetings, events and newsletters;
- 28 lectures from experts were delivered and published – attendance was free of charge and could be booked directly at https://sikkerdigital.dk/national-cybersikkerhedsmaaned/;
- a national awareness campaign aimed at families with 'One click may change everything' as the key message;
- a national awareness campaign aimed at SMEs about general awareness and CEO fraud, encouraging management, especially in small companies, to focus on their own behaviour.

GERMANY

In 2020, 150 partners across Germany used the ECSM in October to participate in nearly 300 events for raising awareness of cybersecurity. The range of events was remarkably diverse this year. There were numerous lectures and employee training courses, but also e-learning courses, interactive social media campaigns, white paper and podcast publications and expert consultation days with individual advice. Against the backdrop of the COVID-19 pandemic, there were also a large number of online offers, such as webinars. Many events gave an overview of the risks and protective measures in cyberspace.

Other key challenges in cybersecurity were also addressed. Several campaigns dealt with the risks in a home office and in digital collaboration and others introduced protection options against phishing attacks and online scams, explained how malware such as ransomware works and gave tips about account protection. Experts were also able to deepen their knowledge on topics such as quantum technology, Industry 4.0 or artificial intelligence. The target groups that the awareness campaign reached out to were noticeably diverse in 2020. Most events targeted company representatives and citizens, with around every 10th campaign targeting academics and media representatives. A small number were also explicitly aimed at teachers.

More specifically, the launch of the ECSM activities in Germany included a virtual conference on 'Networks protect networks' by the Alliance of Cyber Security, which had more than 300 participants. Discussions focused on the topic 'New Work – digital and secure'.

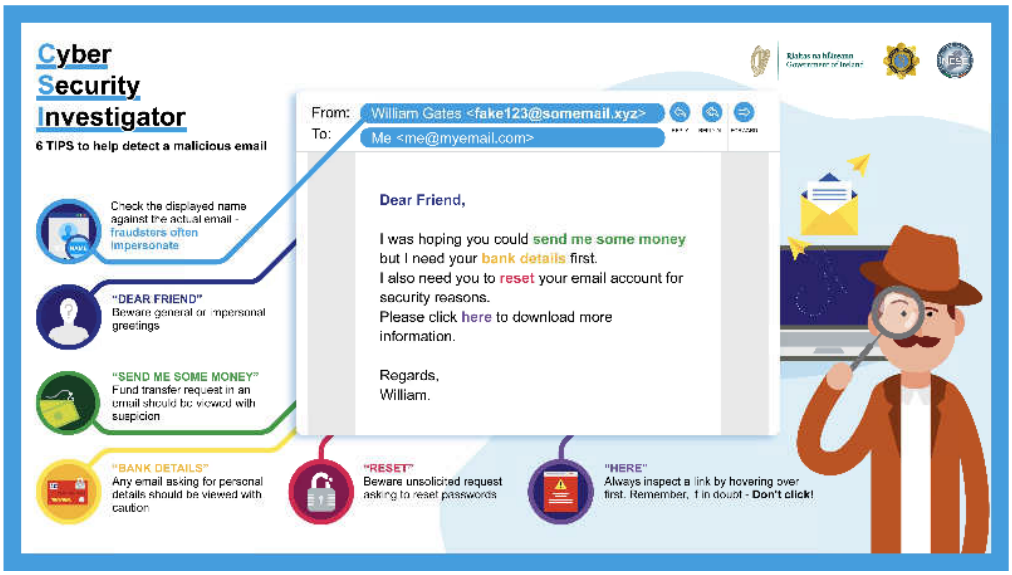
Other activities included:

- awareness raising on 'deep fakes', involving a website containing information on deep fakes, including a short video, as well as a series of three livestreams in cooperation with the Federal Agency for Civic Education (bpb) on truth and relevance in the digital sphere;
- the launch of a new Federal Office for Information Security (BSI) podcast entitled 'Update available' at the end of September, with new episodes released monthly – the podcast focuses on information on cybersecurity for private users;
- publication of a guideline on virtual events – owing to the COVID-19 pandemic, a lot of activities related to THE ECSM took place online and these online guidelines presented information on how to use video conferences safely and how to run virtual events professionally;
- on the German ECSM website (www.bsi.bund.de/ecsm), 151 partners registered 291 activities, 85 % of which took place online and about 10 % focused on the topics of the home office and digital collaboration.

IRELAND

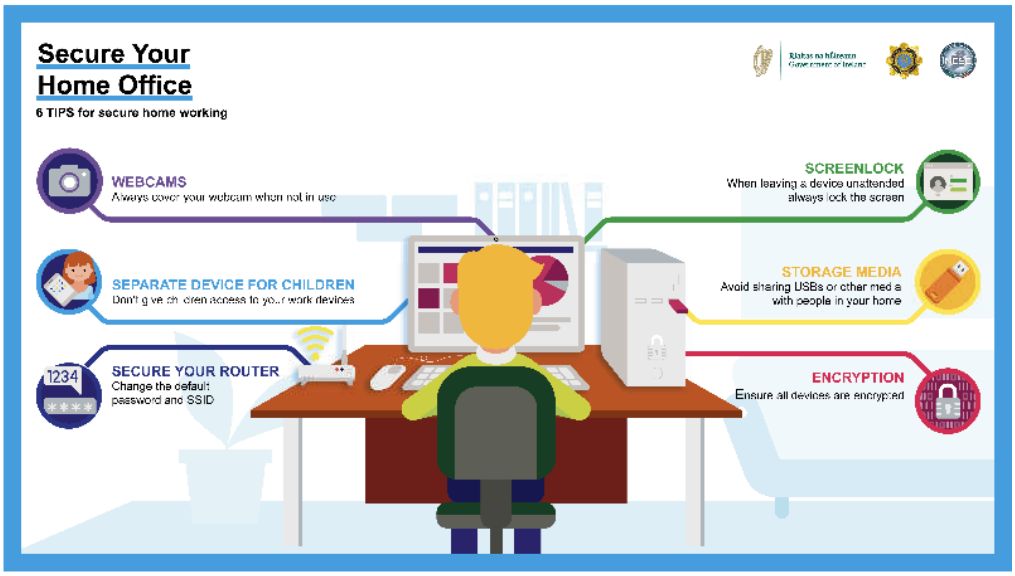
To take part in this ECSM 2020 campaign, the National Cyber Security Centre (NCSC) in collaboration with An Garda Síochána shared their own cybersecurity awareness materials focusing on the overall theme of 'The New Cyber Normal – Working from Home', with subthemes on account security, securing your home office environment and how to spot email scams. The NCSC also promoted content from ENISA on the two themes of cyberscams and protecting your data online with tips on phishing, business email compromise and online shopping fraud, along with personal data protection, cyberbullying and cyberstalking.

Become your own Cyber Security Investigator



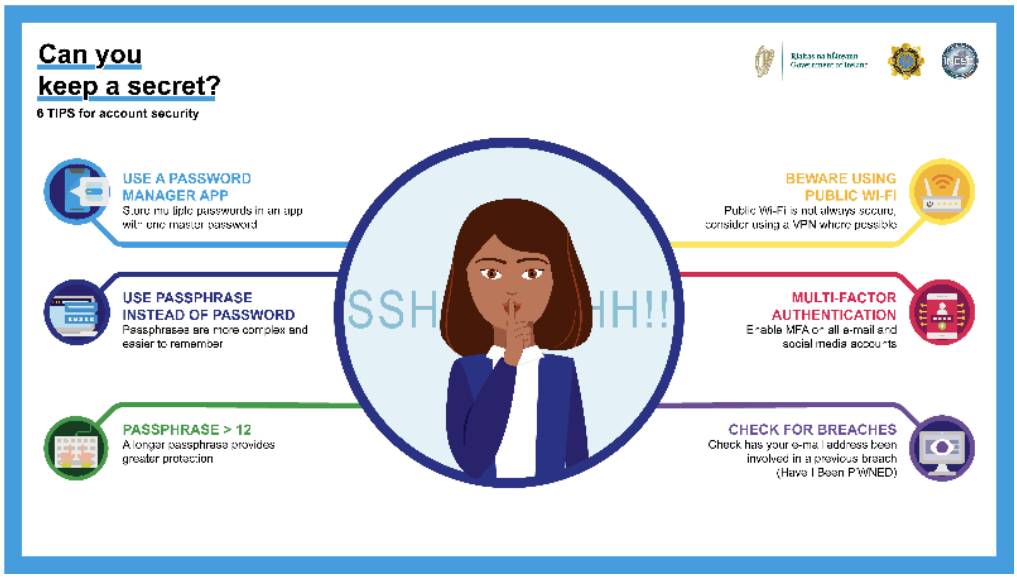
The NCSC also partnered with Cyber Ireland and took part in a webinar on 5G deployment and security in Ireland, which was hosted by Cyber Ireland on 14 October and was attended by over 70 people. The webinar involved an exciting panel, including Joe Stephens from the NCSC's critical national infrastructure protection team, to discuss the advantages of 5G and the need for early adoption in Ireland, as well as the security challenges around the deployment of 5G.

Secure your home office



The department's communications team published a press release for the launch of the campaign and published the NCSC's awareness-raising infographics on the government's 'Be Safe Online' web page (https://www.gov.ie/en/campaigns/be-safe-online/) and on the department's Twitter, Facebook and LinkedIn channels. The NCSC also published the awareness-raising infographics on its own website and Twitter channel. Agencies such as Citizens Information, ICTSkillnet, Webwise and Media Literacy Ireland, among others, were tagged in these publications to allow them to reshare the content on their own social media platforms.

Passwords



ITALY

Under the ECSM umbrella, 43 activities were organised in Italy in 2020.

Most of them were organised by Clusit (the Italian Association for Information Security), a non-profit organisation aimed at facilitating information sharing on information security issues.

Two major events were organised within the ECSM 2020 campaign.

1. Cybersecurity Day 2020 was organised by the Institute of Informatics and Telematics (IIT) of the Italian National Research Council, in the framework of the Internet Festival 2020 week.
   The event was attended by sector experts, researchers and representatives of the business world. The research and innovation activities carried out by the IIT Cybersecurity Lab in cooperation with industry, public administration and law enforcement have been presented in a video exploring the various aspects of cybersecurity that we face every day (https://www.youtube.com/channel/UC9QS3I91xRD8tRISJ_7UlRg).

2. A workshop on 5G security was organised by the Directorate for Communications Technologies and Information Security – High Institute for ICT of the Ministry of Economic Development.
   The workshop aimed at providing a general overview of security and privacy in 5G systems (http://www.isticom.it/).

LITHUANIA

In this year's ECSM 2020 campaign, many cybersecurity events were held:

- the National Cyber Security Centre and the association Window to the Future implemented the social media campaign 'LT Intus', UAB organised an event entitled 'Cyber Security in LT Training', and NRD Cyber Security arranged an International Telecommunication Union (ITU) Centre of Excellence training course entitled 'Building an Effective Cyber Security Team' and organised a meeting of the Lithuanian computer security incident response team (CSIRT) community;
- the Communications Regulatory Authority of the Republic of Lithuania and INFOBALT coordinated an event entitled 'eIDAS Regulation: Electronic Signature and Other Tools for Process Digitisation' and we took pride in closing the event; in addition, a cybersecurity quiz was organised by the National Cyber Security Centre, which assessed the activeness of its participants and highlighted their excellent results (https://www.facebook.com/NKSC).

Throughout October, the National Cyber Security Centre shared cybersecurity tips on its Facebook and Twitter pages.

The Director of the National Cyber Security Centre, Dr Rytis Rainys, said: 'In the field of cyber security, enlightenment and informing forms the first line of defence. Obviously, only an informed user will be able to identify cyber threats and understand what steps must be taken in order to protect himself from cyber-attacks or online fraud. For this reason, the dissemination of information when October has been declared the Cyber Security Awareness Month is relevant at the EU level, as the issue of cyber security is of equal importance in all EU Member States.'

The National Cyber Security Centre is the main Lithuanian cybersecurity institution responsible for the unified management of cyber incidents, for monitoring and the control of the implementation of cybersecurity requirements, and for the cybersecurity of the critical information infrastructure.

LUXEMBOURG

This year, the Ministry of the Economy sponsored a city bus campaign with the ECSM's slogan: 'Cybersecurity – a shared responsibility'.

Cybersecurity Week Luxembourg organised by the Cybersecurity Luxembourg community took place from 19 to 29 October 2020, with 28 sponsors and almost 30 events, mainly held online.

For example, PwC organised a 4-day cycle of digital encounters. New players in the cybersecurity market joined this venture, such as F5 Networks and Fujitsu. Professional associations representing data protection professionals (APDL), the industry (FEDIL) or the world of finance (ABBL) were also present, as well as the Chambers of Commerce and Trades, bringing together European and national decision-makers and SMEs from all sectors. Hack.lu decided to adopt an atypical format, leaving online conferences aside and returning to a more

traditional paper format, with the publication of all of the best papers received in the framework of their competition.

The Cybersecurity Luxembourg Startup Pathway was organised by the Luxembourg Business Angels Network and the Luxembourg Private Equity Association, bringing together the local cybersecurity ecosystem, startups and innovators from around the world. This event was part of the European Startup Competition organised by the European Cyber Security Organisation (ECSO).

An awards ceremony' celebrating five local cybersecurity talents/solutions concluded Cybersecurity Week Luxembourg with a speech by the Minister of the Economy, Mr Fayot, who introduced the latest overview of the Luxembourg cybersecurity ecosystem.

In relation to citizens, the Restena Foundation and the University of Luxembourg held the third edition of the CyberDay.lu, focusing on an online audience of school and university students. BEE SECURE, the national awareness-raising initiative for adults/family, children and students, launched its traditional information campaign, tackling the theme of our private, social and professional 'online image'. Built around the question Bass des sëcher? (Are you sure?), the campaign challenges the user to think twice before posting on the internet. The campaign will run throughout the school period 2020–2021.

ECSM cyber skills and cyber scams material was also shared by the social media channels of the national police.

MALTA

Cyber Security Malta believes that cybersecurity is a relevant topic throughout the year – October is special because all Member States focus their efforts on the same topic and hence the power of collaboration ensures that messages get through more easily. In this regard, Cyber Security Malta organised several awareness and educational campaigns throughout this year that were intended to instil among the Maltese citizens a cyber hygiene culture and a sense of responsibility when utilising the digital world.

Earlier this year, Cyber Security Malta embarked on a project of producing eight short clips depicting the recent adaptions that have been imposed on businesses, employees and citizens owing to the COVID-19 pandemic. Topics such as videoconferencing, teleworking, multifactor authentication, fake news, online shopping and ransomware were addressed. Such clips were aired on the national TV stations (TVM and TVM2) in June and July. It is estimated that around 250 000 people of the Maltese population have seen the clips at least once. Clips were eventually uploaded to Cyber Security Malta's YouTube channel (https://www.youtube.com/watch?v=waZU_llQN7E&t=3s).

Cyber Security Malta has also joined an international alliance with Interpol to promote the 'wash your cyber hands' campaign, with the aim of delivering, on a daily basis, messages to ensure that individuals and businesses are equipped with the knowledge to protect their systems and data. The associated press release can be found on Cyber Security Malta website (https://cybersecurity.gov.mt/resource_articles/20–05–20-malta-joins-an-international-alliance-led-by-interpol-to-enhance-cyber-security-during-covid-19/).

During this year, the Malta Information Technology Agency, through the Cyber Security Malta campaign, launched a secure coding initiative addressed to its employees. Its objective was to disseminate software development material among employees on a weekly basis. This project was launched in July and is expected to continue running in 2021.

The secure coding initiative also took us to the wrestling mat, where the similarities between secure coding and wrestling were explored. These clips were posted on Cyber Security Malta

social media and were aired as a feature during a TV technology programme, Gadgets. Clips are available on the Cyber Security Malta YouTube channel (https://www.youtube.com/watch?v=T0-v6Rx0tHA).

Malta was also an active member of both the ECSM coordination team and of one of the task forces, utilising and promoting the material prepared for the ECSM across the island.

On 28 October, Cyber Security Malta organised the first national cybersecurity webinar, which was entitled 'Emerging Threats... unplugged'. During this 4-hour webinar, executives had the opportunity to explore in depth the anticipated threats for 2021, to discuss cyber protection in a diverse football club environment and to attend a panel discussing the importance of thinking before acting when it comes to cyber protection. Technology workers had the opportunity to follow a live demonstration by Paula Januszkiewicz and, as a conclusion to the webinar, a panel was held focusing on the shifting sands of cybersecurity. There were more than 600 registrations, with a peak of 330 concurrent participants at any one point in time throughout the webinar. The webinar has been uploaded to Cyber Security Malta's social media (https://www.youtube.com/watch?v=maT7CiIBhLw and https://www.youtube.com/watch?v=NrJHQDgdnLs&t=4697s).

NORWAY

The Norwegian ECSM campaign in 2020 was coordinated by NorSIS. The campaign did not follow ENISA's themes for the ESCM as normal. Instead, it was linked to a national scenario exercise entitled 'Digital 2020' as instructed by the Norwegian government. However, as per usual, NorSIS's main aim for the Norwegian cybersecurity month was to create awareness about cybersecurity. Cyberscams and digital skills were a great part of our messages and activities.

Our main activity has been to distribute eight modules of e-learning to employees. These lectures are free for all companies with 20 employees or fewer. We aim to achieve this through a mix of media attention, including social media posts, articles on our website, distribution in our newsletter, participation in seminars, podcasts and attention through other available channels.

Owing to the pandemic, physical meetings and travel have been limited. We therefore launched a video streaming site – Secflix (www.norsis.no/secflix) – as a new channel of communication. It both is targeted at the individual employee or leader and can be used as a tool for information security personnel. Users can distribute a video on a relevant issue to their colleagues, for example.

Results

- Secflix: the site was launched on Tuesday 6 October. The first day it had 55 535-page views.
- In total throughout October, it had 272 222 page views, the average user spent 3,3 to 5 minutes on the page and 80.5 % of the visitors were returning visitors.
- e-Learning: we distributed eight modules of e-learning to 672 companies, 428 of which had 20 or fewer employees and 244 had more than 20 employees.
- Press clippings: 141 press clippings mentioning NorSIS, the national cybersecurity month or other activities in connection with the campaign between 1 and 31 October.
- Facebook: 36 posts were published throughout October. Video posts created the most engagement. ENISA's two videos were the second and third most popular videos. Our activities on Facebook throughout October gained us a reach of 229 613 and engagement in our content reached 32 100.
- LinkedIn: throughout October, we published 26 posts on our LinkedIn page. The majority of the people viewing these posts had a technology background. Although it

normally varies throughout the year, we gained page followers all through the month, ranging from 22 to 36 new followers per week.

- NorSIS website and newsletter: we published 27 news articles on our website and this news was sent to our, approximately, 6 600 subscribers in four newsletters throughout October.

POLAND

The ECSM 2020 campaign in Poland focused mainly on ensuring a social media presence. We were actively running our Facebook and Twitter accounts using materials provided by ENISA and those produced by organisers' initiatives. Furthermore, social media helped us to communicate with our followers and potential organisers of different initiatives. In posts we encouraged the organisation of initiatives and we publicly thanked all participating bodies with weekly updates.

On Facebook, 108 posts were published in the period from 1 to 31 October this year, almost three times more than in October 2019. In this year's ECSM, the total range of organic posts was 70 000. We did not invest in paid reach. Our posts were shared by some of our patrons, including the Polish National Police, which gave us the opportunity to reach many new users.

On Twitter, we published 58 posts and the number of views of all tweets exceeded 23 100. We also had some traditional media impact, mainly in local media.

We accepted and promoted 49 initiatives, of which 24 were school initiatives, raising awareness on different cybersecurity and safety aspects. Other initiatives were organised by public or commercial entities or NGOs. There were many different types of initiatives: lectures, contests or special classes at schools, and conferences, webinars and articles from other entities. One online shop provided a special offer on antivirus software. We are very proud of a successful campaign run by the National Association of Cooperative Banks (an association of local community banks), which disseminated security awareness materials among its clients, who typically are more used to traditional banking methods but, owing to the pandemic, had to switch to online financial activities and needed special guidance and support.

The NASK research institute had also planned its own initiatives but, owing to the pandemic and some political tensions, those activities were postponed. We are planning to deliver them in the next few months, and these will also use the ECSM social media for promotional purposes.

During the pandemic, the cybersecurity topics were very engaging for schools and organisations supporting teachers. The ECSM could be a very good supplement to the actions of Polish Safer Internet Centres. With the ECSM in October and Polish Safer Internet Day in February, there would be a year-round focus on security and safety issues for the educational community.

The objective for our national campaign is to actively run our ECSM social media all year round to build a community that is interested in cybersecurity and also to disseminate security awareness materials produced by ENISA, our colleagues from other countries and international organisations such as Europol and Interpol. We believe that October should be a culmination of the yearly efforts.

We very much appreciated the materials and all of the engagement from ENISA. Without ENISA's support, the campaign would be less active and effective.

PORTUGAL

The Portuguese National Cybersecurity Centre (CNCS), like in previous years, carried out an awareness campaign within the scope of ECSM 2020. This year, Portugal focused on having a very active media and social media presence online and its collaboration with ENISA helped to achieve this goal.

Two campaigns consisting of various infographics on good practices in cybersecurity were organised. The first campaign, called 'Popular wisdom can help', included 14 posts in the national language and the second was a campaign developed in partnership with the National Order of Psychologists, consisting of four posts with different key messages, and addressed the topics of cyber skills and cyber scams.

Partners were challenged to create videos with testimonials and examples of cybersecurity best practices related to cyber skills. Those videos were published on our social media channels.

Additional activities and achievements included the following.

- An article about the ECSM was published in a magazine.
- The Safe Internet Centre aimed at younger audiences, parents/educators and the elderly joined forces with the CNCS and jointly sent a kit with printed promotional material to all CIS partners.
- A survey was developed and disseminated to teachers (although not in preschools) about the constraints of teleworking. This survey was available between 20 October and 15
- November throughout the country and was supported by the Ministry of Education, receiving a total of 21 126 responses. The results will be announced at a conference that is to be held in December.
- A special edition of our general cybersecurity course was delivered to CNCS's partners on 28 and 29 October (which had more than 200 participants).
- A variety of online events, including awareness-raising activities, were delivered by national campaign partners: conferences, workshops, talks and other initiatives. The total number of participants in these activities reached up to 600 citizens.

ROMANIA

The Romanian national campaign focused on having a very active media and social media presence online. The collaboration with ENISA helped us to jointly manage and organise more efficiently our official communication channels, and disseminate awareness material in our national language. This collaboration saved us time and enabled us to focus on what others were doing, in order to help magnify the message.

For the cyberscams campaign theme, we teamed up with Europol and the Romanian police to reuse and update the scams awareness material of ECSM 2018. The amount of content on cyberscams was doubled in this ECSM, with materials from CS TF also used. The outcome was very satisfying, as we received good engagement on social media and many people were interested in if the materials could be downloaded and disseminated better.

Moreover, in recent years, we have noticed that, through our press monitoring, a lot of media channels followed our social media accounts very closely and generated news from what we posted. This trend continued in ECSM 2020. Most of the ENISA or Europol materials were published by the press, linking them to the Romanian National Computer Security Incident Response Team (CERT-RO) articles on cybersecurity awareness.

Our close collaboration with the press paid off. AGERPRES (a news agency) and Romanian national radio closely followed our activity during the ECSM and supported it. Via AGERPRES, a lot of the ECSM news reached local or national media. In addition, we had two slots on

Romanian national radio, during which we talked about cybersecurity awareness and issued advice for common users (see https://youtu.be/GFv9D98I4gM).

Furthermore, we invited to several interviews at different television channels for promoting awareness. We also gave talks about the ECSM activities at the cybersecurity conferences or events at which we were invited to speak, including certCON 10, the CERT-RO annual international conference on cybersecurity, which had a separate panel on education and awareness. At that conference, we touched on both topics of ECSM 2020: cyberscams and digital skills. Our online audience for the event was over 400 participants.

On the topic of digital skills, we teamed up with our partners from certSIGN to deliver, at the national level, an awareness campaign called #Cyber4Kids that targeted children, parents and teachers. In parallel, we also engaged with the Ministry of Education and with regional educational bodies. We held a mini online series, supported by materials (guides) in Romanian and English, that can be downloaded online or offline and disseminated further (see https://www.certsign.ro/ro/cyber4kids).

We also partnered with the cyber division of the Romanian Secret Service (Cyberint) to deliver a national anti-ransomware awareness campaign, which was included a video tutorial on how to avoid ransomware and what to do if you ever get infected (see https://youtu.be/WzKhf1b6Tro).

Another topic we worked on and on which we generated awareness material including guides and video tutorials was the EMOTET malware, which has recently proven to be a real issue for companies, institutions and even common users in Romania (see https://youtu.be/eqbdi_i8hfw).

Last but not least, the Romanian Cyber Security Challenge (RoCSC) was organised as an ESCM 2020 activity. RoCSC is an annual CTF event organised in Romania to reward local best practices in cybersecurity; there are both juniors (16–20 years) and senior (21–25 years) categories. The national competition replaced what was supposed to be the final stage of ECSM 2020, which has been postponed until next year.

SLOVENIA

For this year's ECSM, the campaign of the Slovenian Computer Emergency Response Team (SI-CERT) primarily centred on an online stand-up show entitled 'Splet naključij' (Web of coincidences) featuring some of the most prominent Slovenian stand-up comedians. The main performers of the shows were two Slovenian stand-up comedians, who hosted a famous Slovenian guest on every show. Each show presented a different online scam and offered solutions to help users recognise and protect themselves against scammers.

The show comprised four episodes that were streamed on Varni na internetu (Safe on the internet) social media channels (Facebook and YouTube) every Thursday in October. Each episode featured a short, humorous sketch that was later uploaded to our Instagram channel. To further promote our campaign, we filmed three short teasers that were streamed across our social media channels and promoted on YouTube (a YouTube playlist with all of our ECSM-related videos is available here: https://www.youtube.com/playlist?list=PLUVdjpfSn3X-xKE4Ja_APsc0Axc7WMLt4).

Each video was branded with the ECSM logo, like all other visual materials and press releases.

All four episodes were viewed more than 230 000 times on YouTube and more than 53 000 times on Facebook. In October, we achieved a total reach on our Facebook page of 600 000, which was a great success and helped in promoting ECSM idea and values.

All of our materials were promoted on social media (promotional videos and paid advertising) as well as offline (PR activities, advertisements on national radio stations, and TV and radio statements). We even had a slot on a radio show that was dedicated to identity theft on the commercial radio station with the highest ratings in Slovenia. In addition, we wrote an article about advanced ransomware attacks for GÉANT and for the ECSM-dedicated edition of their newsletter, Connect (see https://connect.geant.org/2020/10/19/advanced-ransomware-attacks).

SPAIN

In the light of the ECSM campaign, Spain organised a series of activities to promote an awareness of and a culture in cybersecurity.

There were several organisations involved, such as the National Institute for Cybersecurity (INCIBE), the National Cryptologic Centre (CCN), the National Security Department, the Joint Cyber Command, the National Centre for Critical Infrastructures and Cybersecurity (CNPIC), the law enforcement agencies, regional CSIRTs and others.

Several national CSIRTs created specific web pages dedicated to the ECSM, namely INCIBE and CCN, which provided specific material on this year's topics. The awareness-raising material (videos and infographics) were translated into Spanish.

With regard to the private sector, many events were also aligned to ECSM 2020. These organisations and companies helped to share our information by using their communication channels (e.g. their websites and social networks).

A total of 27 activities were undertaken and promoted through the ECSM website, with a particular highlight being ENISE Spirit, the annual cybersecurity conference organised by INCIBE (which this year was a video conference). Additional activities were also organised including training courses, workshops, conferences and awareness-raising sessions, and some guidelines and multimedia materials are expected to be released soon.

Spain also approved the National Cybersecurity Forum, a public–private initiative that formed part of our National Cybersecurity Strategy 2019. This forum focuses on creating synergies and in particular on generating knowledge regarding opportunities, challenges and threats to security in cyberspace. The forum incorporates representatives from civil society, experts and individuals from the private sector, academia and various associations. The main factors that it

addresses are culture, strengthening industry, research, development and innovation, and promoting talent and education.

The forum was an important element in ECSM 2020, helping to spread key messages and encourage participation in activities.

SWEDEN

The Swedish team is very proud to have conducted a successful campaign in spite of the ongoing pandemic. Owing to the circumstances, we concluded that the campaign was even more necessary than usual. In this year, we believed that joining forces with other organisations would send a powerful message of unity and would enforce that cybersecurity is a shared responsibility. It is also an effective way to communicate. Owing to the situation this year, we were obliged to revamp campaign materials from last year.

TÄNK SÄKERT

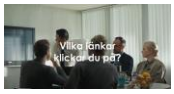
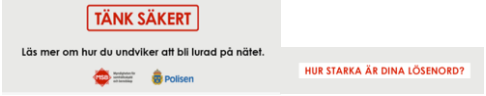
Ett samarbete mellan:

MSB Myndigheten för samhällsskydd och beredskap Polisen

The 2020 'Tänk säkert' campaign was coordinated at the national level by the Swedish Contingency Agency (MSB) and the Swedish Police Authority in close collaboration with Swedish organisations from the public, private and non-profit sectors. This year, we focused even more on municipalities and regions when raising awareness and conducting activities during the month.

The main objective of the campaign was to help individuals and small businesses (with 0–10 employees) to develop routine cyber hygiene habits. To achieve this, we described some of the most common threats online and provided simple, hands-on recommendations on how to avoid malicious attacks such as phishing and ransomware, credit card fraud and passwords. The motto was 'Skydda din väg in' (Protect your points of entrance).

Described below are some of the highlights of the 2020 Tänk säkert campaign.

Campaign website https://www.msb.se/tanksakert	• Campaign materials such as a campaign video, checklists and an ECSM video and infographic
Campaign video https://www.youtube.com/watch?v=4snShZAmvtU 	• A 16-second video consisting of a humorous scene from an office environment (a revamp from 2019) • The campaign announcement shows, which reached 92 000 people
MSB and Swedish Police Authority – Facebook, Instagram, Instagram Stories and LinkedIn	• Total reach: about 1 million
Programmatic display advertising 	• Click through rate: 17 %

Activities; MSB and Swedish Police Authority 	• MSB conducted a series of webinars during which participants discussed the company's cybersecurity awareness • The Swedish Police Authority produced four videos, each 30 seconds long, which were published on social media
Partner activities 	Some of the activities conducted during the ECSM month: • a great number of internal and external digital activities, such as seminars, newsletters, podcasts and advertisements • more than 30 webinars, with presentations given all over Sweden • many articles published on websites and in printed media • the podcast #Blisäkerpodden #89, #90, #91 • a campaign video shown on screens at, for example, 292 Handelsbanken offices
Survey targeting the public conducted by Enkätfabriken at the request of MSB (1 083 interviews) – September 2020 https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/informationssakerhetsmanaden/tank-sakert/msb-enkatundersokning-itsakerhet-tanksaker2020.pdf	Some of the findings include the following: • 50 % of the respondents increased their digital presence during COVID-19 • 7 % reported an increased worry of being exposed to IT-related crimes • only 8 % have taken precautions against IT-related crimes

SWITZERLAND

The following are the highlights of the Swiss ECSM 2020 campaign activities, with useful links listed.

Website

- Topic: Malware
- Address: https://www.ibarry.ch/en/safe-surfing/malware/
- Social Media: Facebook, Instagram

Print

- Stickers
- Face masks
- Sent to ca. 220 organisations

TP-AL-21-001-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, please visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-466-4
DOI: 10.2824/224495