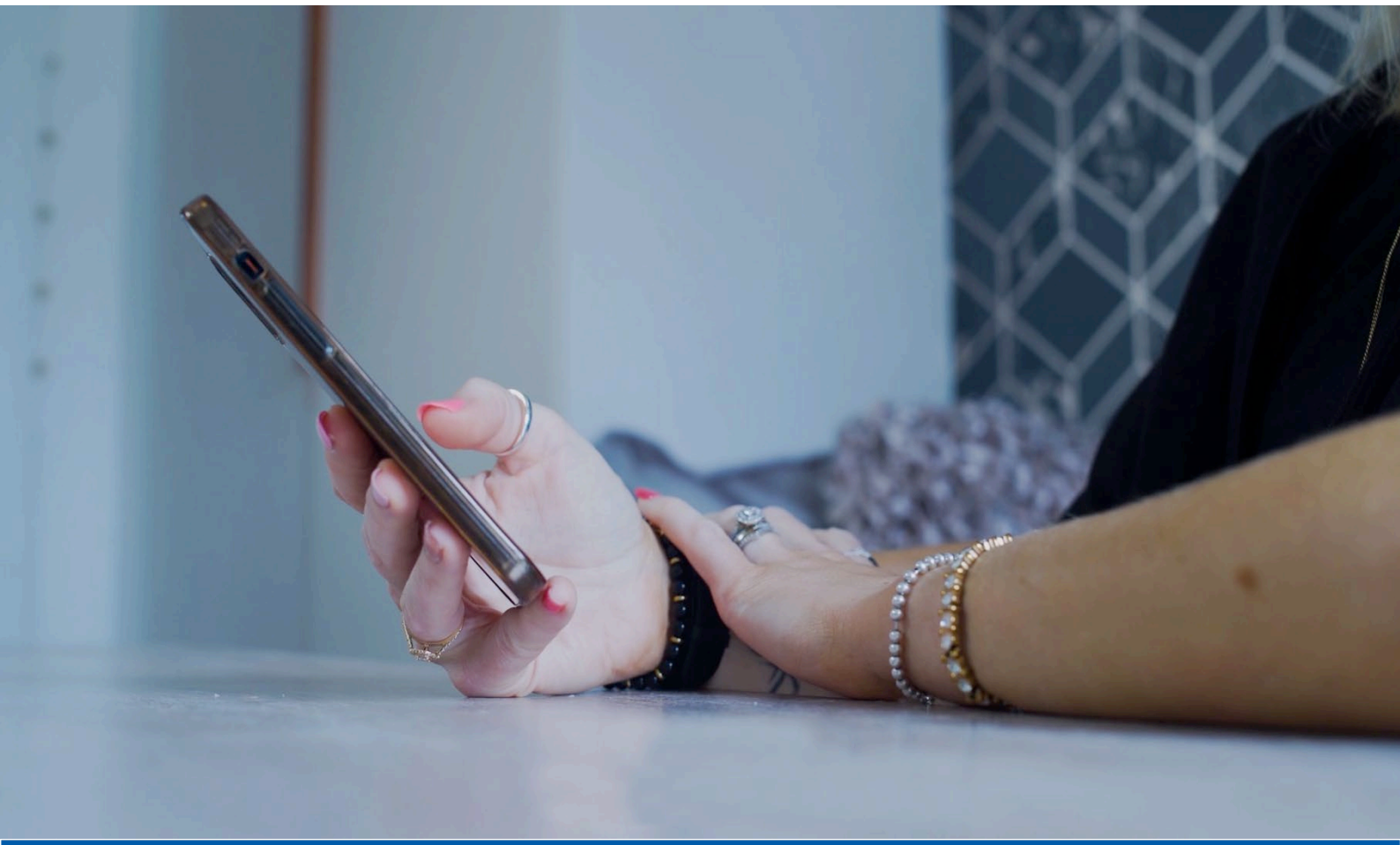
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



EUROPEAN CYBERSECURITY MONTH (ECSM) 2021

MARCH 2022

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. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

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

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

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

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2022

This publication is licenced under CC-BY 4.0

"Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/).
This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

Cover image © 2021, ENISA

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-573-9, DOI 10.2824/647127, ISSN:

EXECUTIVE SUMMARY

The ongoing COVID-19 pandemic has driven more people to work, share and shop in cyberspace, accelerating a migration to online existence that began in 1989 when the world wide web came into being.

ENISA has been raising public awareness of cybersecurity risks through an annual EU-wide awareness-raising campaign since the idea was explored in a feasibility study in 2011 and launched as a pilot project in 2012. Aimed at citizens, organisations and businesses, the European Cybersecurity Month (ECSM) is a month-long campaign held every October across the EU and beyond. ECSM promotes cybersecurity awareness and education, and provides guidance on good practices for individuals and organisations in order to increase resilience and create a more cyber secure culture across the EU.

Importantly, 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, ENISA must promote a high level of cybersecurity awareness, including cyber hygiene and cyber literacy among citizens, organisations and businesses.

The COVID-19 pandemic certainly changed the scope of the ECSM back in 2020. Up to that point, the ECSM had mainly been an interactive month with physical events spread across participating countries. The pandemic posed a great challenge to staging the workshops, conferences, training sessions and other events that made up this platform for sharing ideas and campaign materials. However, ENISA was up for the challenge and succeeded in transferring to a digital platform, accelerating its digital transformation. The 2021 European Cybersecurity Month Campaign was built on the solid foundations of that previous experience and success. The aim this year was to go beyond informing and to encourage action and behaviour change.

Building on the analysis of what worked well in the 2020 campaign, **more video** was used to generate greater engagement. A series of **real-life stories** were accompanied with actionable recommendations. **Infographics** were created and distributed through social media with a view to helping the viewer take action if needed. **Gamified content** such as social media puzzles were included to engage people in innovative ways. This strategy ensured that ENISA built on the success of last year with the high impact 'Think Before U Click' campaign. The ECSM 2021 campaign was a resounding success this year with significant growth in social media mentions overall, and social media reach at over 20 million (over twice the 8.8 million figure of 2020). Twitter, a powerful tool for reaching the campaign's target audiences, showed a 15% growth in followers. In fact the @CyberSecMonth account now has well over 28,000 followers. Over 70% of MS say that their campaign (or their partners') has had an impact in reducing cyber incidents.

Highlights of the 2021 ECSM Campaign

Number of **activities bounced back to 517** after dropping off at the start of the pandemic

Percentage of member states agreeing that their or their partners' campaigns reduced cyber incidents **was very high at 73%**

Online social media reach of ECSM content increased to **over 20 million** (from 8.8 million last year)

Proportion of member states that gave ECSM a **"good" or "excellent" rating was 69%**

Social media mentions increased to **over 23,000** (a 3x increase on 2020)

Number of Twitter followers increased to **over 28,000** from 24,000

Beyond the effectiveness of the campaign content itself as shown in the highlight figures above, ENISA sought to find a better way to measure effectiveness in terms of metrics related to behavioural change. This meant finding new and better ways of collecting data on the activities at Member State level. Data collection from the Member States was also improved following on from the analysis of ECSM 2020 and taking on board the feedback from the national coordinators themselves. The evaluation questionnaires provided to Member States, to analyse the event after the fact, were updated to make them more scientifically accurate while also allowing greater flexibility and more insight into the perspectives of key coordinators of the Member States in the qualitative data gathered. More countries participated in the evaluation this year (at 26) than for any previous ECSM.

ECSM 2021 was more evolved in terms of output, participation and analysis than any previous European Cybersecurity Month. In the coming years, ENISA and all Member States will need to continue engaging citizens and organisations in boosting cybersecurity awareness and education. 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 future. This discussion is essential to ensuring that the European Cybersecurity Month will continue to evolve with a focus on addressing the growing needs of individuals, organisations and businesses across the EU.

TABLE OF CONTENTS

1. INTRODUCTION 6

1.1 THE ECSM STORY 6

1.2 TARGET AUDIENCE FOR THIS REPORT 7

1.3 EVALUATION METHODOLOGY 7

1.4 THE STORY OF ECSM OVER THE YEARS 8

2. PLANNING PHASE 9

2.1 ROLE OF ENISA AND MEMBER STATES IN ECSM 2021 9

2.1.1 The ECSM Vision 9
2.1.2 The ECSM Mission 9
2.1.3 Objectives for ECSM 2021 9

2.2 COORDINATION 10

3. CAMPAIGN PLAN 12

3.1 THEMES OF ECSM 2021 AND RATIONALE FOR THEIR SELECTION 13

3.1.1 Be Cyber Secure from Home 13
3.1.2 Cyber First Aid 13

3.2 ECSM 2021 TARGET AUDIENCE PERSONAS AND RATIONALE FOR THEM 14

Women in particular are juggling work and home responsibilities including home schooling. 14

3.3 ECSM 2021 COMMUNICATIONS CHANNELS 15

4. EXECUTION PHASE 17

4.1 CONTENT CALENDAR 17

4.2 LAUNCH OF THE ECSM 2021 18

4.3 CAMPAIGN MATERIALS AND SOCIAL MEDIA CONTENT 19

4.3.1 Be Cyber Secure from Home 19
4.3.2 Cyber First Aid 20

4.4 CAMPAIGN STORIES 21

5. EVALUATION 23

5.1 FOCUS OF MEASUREMENT 23

5.2 QUESTIONNAIRE OPTIMISATION 23

5.3 ASSESSMENT OF IMPLEMENTED ACTIONS BASED ON THE EVALUATION METHODOLOGY 24

5.3.1 Results of Member state EUSurvey Questionnaire 24
5.3.2 Results of Member State Web Activities 34
5.3.3 Results of Member State Social Media Activities 34

5.4 ASSESSMENT OF WEB RESULTS 35

5.4.1 Assessment of ECSM Website Results 35
5.4.2 ECSM Map of Activities 36
5.4.3 ECSM Interactive Map 37

5.5 ASSESSMENT OF MEDIA MONITORING RESULTS 38

5.6 ASSESSMENT OF ENISA SOCIAL MEDIA RESULTS (ORGANIC AND PAID) 39

5.6.1 Daily growth of Twitter @CyberSecMonth followers 39
5.6.2 Annual number of Twitter followers of @CyberSecMonth 40
5.6.3 Social media reach 40
5.6.4 Daily Mentions 41
5.6.5 Twitter Follower Demographics 42
5.6.6 Top Keywords 43
5.6.7 Top Entities 43
5.6.8 Sentiment 44
5.6.9 Emotional Comparison 44
5.6.10 Top Hashtags 44
5.6.11 Number of campaign hashtag mentions per country on a worldwide scale 45
5.6.12 The Power of Twitter 46
5.6.13 Emoji usage 47
5.6.14 Gender Breakdown 47
5.6.15 Paid post results 48
5.6.16 Comparison between previous years for the social media campaign effectiveness 49

6. CONCLUSIONS AND RECOMMENDATIONS 50

A ANNEX: MULTIMEDIA CONTENT SAMPLES 51

B ANNEX: CONTENT CALENDAR EXAMPLE 62

C ANNEX: CAMPAIGN STORIES 64

1. INTRODUCTION

1.1 THE ECSM STORY

When ENISA was established in 2004 few could have imagined how important it would be for people, businesses and institutions to have security in cyberspace. ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, engages Member States and collaborates with them and with EU bodies, and helps coordinate a European response for the cyber challenges of tomorrow.

ENISA is committed to increasing awareness of cybersecurity across Europe by providing up-to-date digital security information on cyber threats to all Europeans each October through the European Cybersecurity Month (ECSM) campaign.

A feasibility study for ECSM was carried out in 2011 and the first ECSM campaign was launched as a pilot project in 2012. This was the genesis of what was to become the EU's annual month-long campaign dedicated to promoting cybersecurity among citizens and organisations. This is achieved every year by providing up-to-date online security information through awareness raising and sharing best practice across Europe.

Each year, for the entire month of October, hundreds of activities take place across Europe with 517 activities registered and approved in the ECSM website for 2021. These activities include conferences, workshops, training sessions, webinars, presentations and much more, all organised to promote digital security and cyber hygiene. For the first time this year, steps were taken to promote ECSM throughout the year by also running a promotional campaign about it in June.

The ECSM gives ENISA the opportunity to raise awareness of cyber threats within specifically identified target groups by engaging directly with EU citizens (the end users) as well as businesses (the middlemen). This is done with partner organisations as well as, for the first time in ECSM 2021, ambassadors, well-known individuals and competition winners. The goal of ENISA is to build on this shared knowledge and together advance cybersecurity on all fronts.

To help create a Europe fit for the digital age, people need a strong knowledge of cybersecurity and good cyber practices which means we need to further build trust among EU citizens. Being aware of cyber scams and "thinking before you click" are part of the ECSM's easy-to-follow advice to limit risks and support us in securing this trust.

Click here to watch the ECSM 2021 campaign "coming soon" video

In the last two years, the COVID-19 pandemic has meant that Europe has changed in a very significant way. As people and institutions across the EU found a way to respond to the pandemic more and more EU citizens found themselves working and socialising in cyberspace. More people online means more vulnerable people falling prey to cybercrime. New generations brought up around cyberspace may offer better innovations for cybersecurity through their knowledge and skills, but more sophistication also means a growing industry of cybercrime.

Europe in 2021 is very different to the Europe of 2012 when ECSM was first launched. All through the years since that first ECSM campaign took place in 2012, it has adapted to the changing environment and the needs of its target groups — going from strength to strength. The ECSM initiative is coordinated centrally by ENISA who works in close collaboration and deep engagement with the Member States.

ECSM directly meets the agency's brief of raising cybersecurity awareness for EU citizens across all Member States, making their digital world safer as they navigate their cyber life.

1.2 TARGET AUDIENCE FOR THIS REPORT

This report summarises the activities carried out by ENISA, as well as participating EU Bodies, Member States, EFTA countries and partners for the 2021 campaign. It presents the evaluation of the campaign as well as insights that can be drawn from it for future years.

This report is intended for organisations that have supported the ECSM - or intend to do so in the future. The report may also be of interest to cybersecurity professionals and other groups who have participated in ECSM. The report is also useful to EU and national policymakers who are aiming to improve the cybersecurity awareness of citizens and professionals.

In addition, this report is publicly available to any EU citizen with an interest in ENISA, ECSM or cybersecurity in general to help them understand what initiatives took place during the 2021 European Cybersecurity Month and its results.

1.3 EVALUATION METHODOLOGY

European Cybersecurity Month continues to grow in strength. Year after year the impact is wider and larger in terms of the different audiences it reaches and the number of clicks, tweets and video views that it generates. As the evaluation methodology evolves over time, this year ENISA determined that there was a need to start moving towards trying to measure behavioural change. This led us to look beyond the previous Key Performance Indicators (KPIs) and explore if we could start introducing some different performance indicators that could in the medium to long term show us whether there has been behavioural change in the target groups.

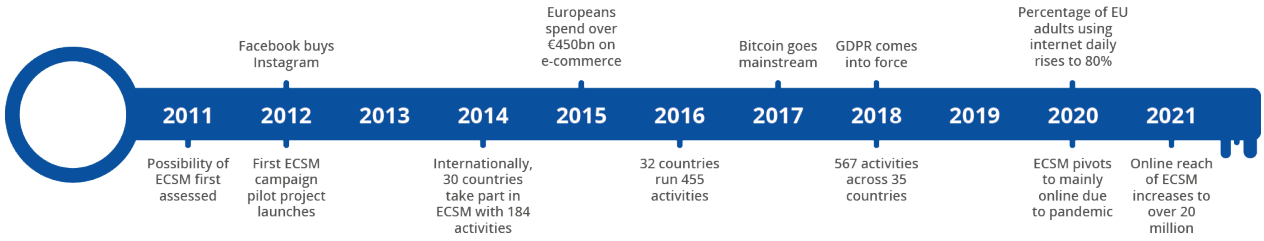
This is something that ENISA has been doing together with a dedicated new task force to develop KPIs which focus more on the behavioural side. The focus is to look at the end user outcomes of the campaigns and try to measure them - as opposed to just measuring the communications outputs. Whilst measuring the behaviour at citizen level has been a difficult challenge for European level initiatives, collaboration with Member States can offer transparency through access to partner organisations and users.

Awareness raising is an indispensable component of improving cybersecurity within the EU. However, this is a very big challenge. Many incidents are enabled by some type of human error, and there is a strong human factor at play in prevention, making cybersecurity everyone's responsibility. Changing behaviour is therefore an essential component of building a Europe fit for the digital age. Improving and evolving the way that the impact of ECSM is measured to include behavioural change is essential. Before organisations can go about changing behaviour through campaigns, research needs to be done to understand what the current status quo is. That is, research should look into what the attitudes, capabilities, and challenges are for users that may be preventing them from adopting cyber hygiene best practices.

1.4 THE STORY OF ECSM OVER THE YEARS

Since being launched as a pilot project in 2012, the ECSM campaign has been coordinated by ENISA and the European Commission with the support of EU Member States and many partners. Governments, universities, think tanks, NGOs, professional associations and private-sector businesses from Europe and beyond join the campaign each year to unite people across the EU against cyber threats. Not only does the campaign promote the safer use of the internet for EU citizens, but it also strives to provide ready access to the knowledge and tools to do so. ENISA coordinates the organisation of the ECSM campaign by acting as a "hub" for all participating Member States and EU institutions. ENISA does this by providing expert suggestions, generating synergies and promoting common messaging among EU citizens, businesses and public administration. A crucial aspect of this is that we publish new creative content and provide expert advice on different cybersecurity topics for stakeholders in Member States to use at a local level.

Timeline of ECSM and Key Internet Milestones



2. PLANNING PHASE

2.1 ROLE OF ENISA AND MEMBER STATES IN ECSM 2021

2.1.1 The ECSM Vision

ENISA through ECSM aims to create a cybersecurity culture across the European Union.

Through ECSM, ENISA develops innovative and engaging ways to raise EU citizens' awareness of cybersecurity and enhance the pan-European vision of stronger cybersecurity by promoting collaboration with the EU institutions, Member States and international organisations.

2.1.2 The ECSM Mission

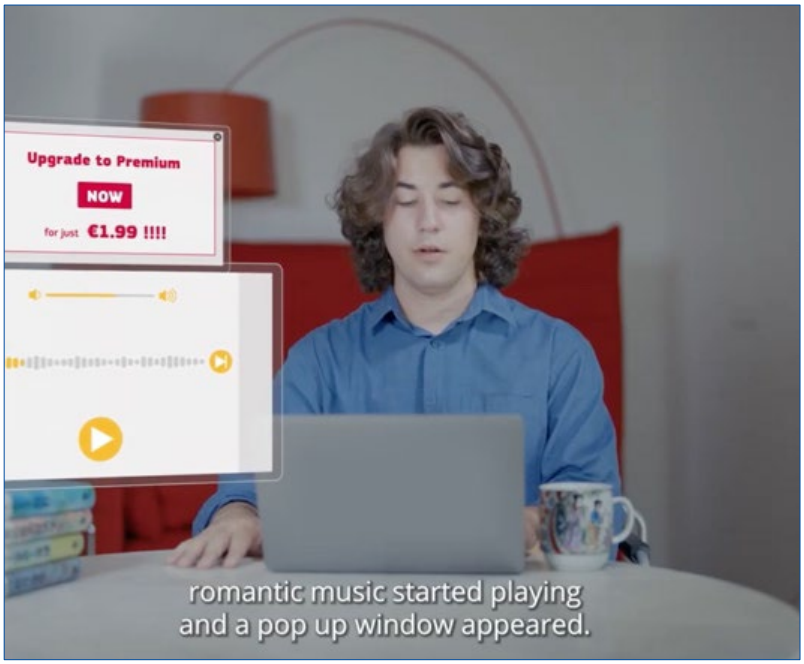
The Agency's mission for the ECSM is to collaborate with the EU institutions, Member States and international organisations by finding innovative and fun ways to raise EU citizens' awareness of cybersecurity and enhance the pan-European vision of stronger cybersecurity.

Watch Juhan Lepassaar, ENISA's Executive Director, introduce ECSM 2021

2.1.3 Objectives for ECSM 2021

The key objectives of the 2021 ECSM campaign were:

- generate general awareness about cybersecurity;
- educate and enhance awareness of information security and privacy by increasing awareness on the chosen themes of 2021 campaign across the EU;
- elevate the understanding of cybersecurity risks and practices across the EU and globally;
- promote the safer use of the internet for end-users and the practice of basic cyber hygiene;
- continue building on the strong track record of this annual campaign in raising awareness of cybersecurity across Europe;
- engage relevant stakeholders and increase the participation of EU Member States;
- increase media interest and political interest at EU and national levels through a Europe-wide campaign and through national campaigns.



ENISA'S ROLE

Through ongoing advocacy, communication and engagement, ENISA's work in organising the ECSM 2021 campaign supports the agency's overall ambition of creating empowered and **engaged communities across the cybersecurity ecosystem**

2.2 COORDINATION

Coordinating a campaign of the scale of ECSM across EU member states, EFTA countries, the European Commission, Europol and the European Central Bank amongst others in a global pandemic was always going to be a challenge. On-going and effective communication with all stakeholders across the group was essential to ensure the success of ECSM 2021.

As described in more detail below, ENISA led regular communication with Member States to enhance collaboration and cooperation across all involved. Using online platforms such as Webex effectively was key to the planning and exchange of ideas. The Campaign Coordinators (CG) group was the high-level planning committee. This group included all member states, EFTA countries, representatives from the European Commission and other important partners like Europol. The CG typically met monthly on video conference calls, with voting on any topics taking place within the chat as necessary in order to streamline decision-making.

Four Task Forces were created, each focussing on a different topic: one each for the two themes of the campaign, one for the governance model and one for reviewing the evaluation framework. Each of these task forces met regularly and reported back on the main "CG" meetings. These meetings were all highly interactive using video and screen sharing as well as the chat function to foster open and productive communication. At both task force and CG level, a mix of tight focus and big picture kept the momentum going and gave everyone a voice at the planning meetings.

Campaign coordinators exchanged ideas for 2021 and information from previous campaigns in an open and positive way sharing lessons learned and best practices. Working closely with them, ENISA was able to finalise key areas of the campaign, such as the themes of the month, the creative content, and the organisation of the campaign content calendar.

Here is a good example of content from Europol:

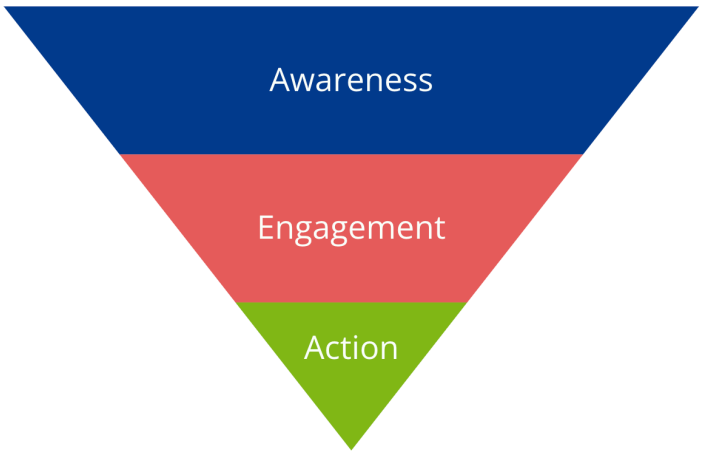
3. CAMPAIGN PLAN

This year's ECSM campaign was designed to address security issues surrounding the digitalisation of everyday life, accelerated by the COVID-19 pandemic. Of course, because of the pandemic the majority of this year's ECSM activities – from conferences and training to presentations and knowledge games – have moved online.

Overall, the move towards everything now being digital influences all the target audience's interactions with cybersecurity as a topic in 2021. The ECSM was an opportunity to promote the underlying value that is the foundation of the ECSM, namely that cybersecurity is a shared responsibility. Following on from 2020's campaign, and encouraging people to 'Think Before U Click' as a motto for a second year, the 2021 campaign highlighted different cybersecurity themes to help users identify and prepare for cyber threats.

An online ECSM coordinators group planning meeting was held in March 2021. Reflecting on last year's successes and learning points the group also set to the task of identifying themes for the 2021 campaign. The group agreed that there would be four Task Forces (TFs) this year: one for each of the two themes, one working on a governance model and terms of reference, and one reviewing and improving the evaluation and metrics framework. This latter task force on evaluation included looking at parameters related to behaviour change.

A number of different potential areas of focus were identified by the group prior to the meeting using a survey. Among the themes considered were phishing, securing SMEs, communications security, identity theft and security in healthcare among other topics. The pros and cons of these were discussed during the planning meeting. While all of these themes were given consideration two themes were agreed on as being the main focus for 2021 "Being Cyber Secure from Home" and "Cyber First Aid" for the reasons summarised below. These are the two themes that would define the content for the two phases of ECSM and which were executed using a campaign strategy that included the funnel approach shown below:

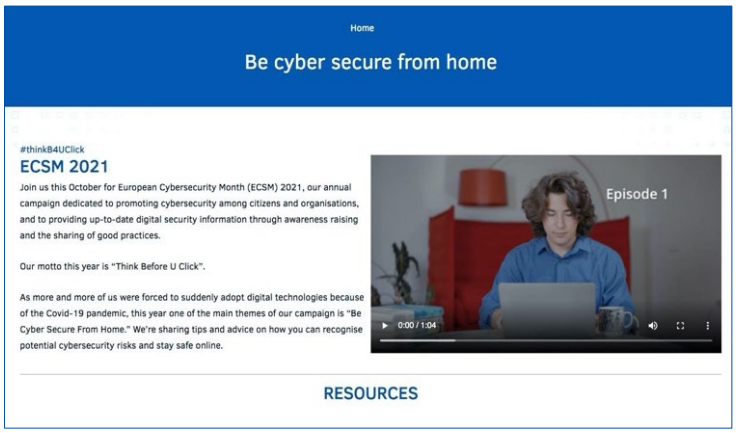


3.1 THEMES OF ECSM 2021 AND RATIONALE FOR THEIR SELECTION

3.1.1 Be Cyber Secure from Home

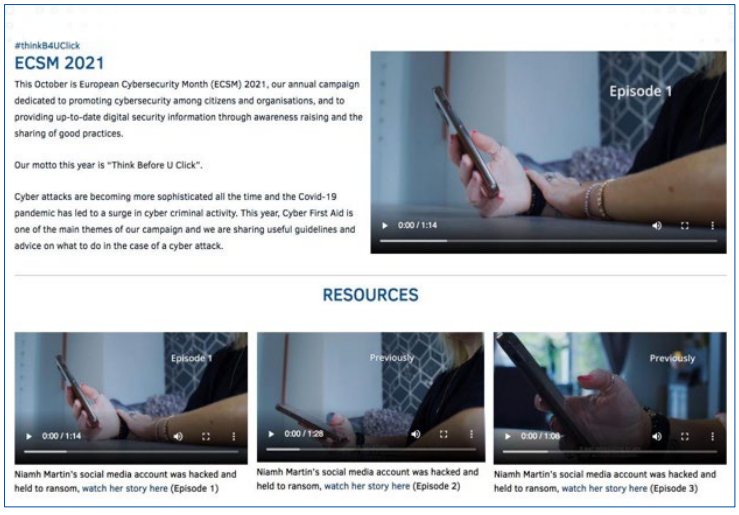
The first theme centred around “Being Cyber Secure from Home” by providing tips on how one can remain cyber secure when working, studying or corresponding online from home. The theme aimed to promote cyber hygiene and good practices online.

Although the coordinator group felt that there is a lot of information already available on this topic, during the planning meeting it was agreed that there were still a lot of areas for improvement. It was agreed that refreshed messaging that was updated to include current best practices and real life examples would catch the attention of the public. The dedicated task force assigned to this theme took on this opportunity to collect key messages and update them; including tips on best practice, real life examples and incidents. For this theme “Be Cyber Secure from Home” it was also important to note that different aspects of this affect men and women differently.



3.1.2 Cyber First Aid

The aim of the theme of Cyber First Aid was to provide guidance to citizens who fall victim to cyber attacks. This theme appealed to most of the coordinators at the planning meeting as it was not dealt with in any of the past campaigns, and there was agreement that a large proportion of the EU population does not know where to turn to in the event of a cyber-incident. Sharing guidelines on what to do in case of online fraud or other cyber-security incidents would therefore add value and help achieve the campaign’s objectives.



The goal was to encourage users to have a heightened awareness of the most common cyber threats and provide advice on how to react in case one falls victim. To facilitate this, an EU map with contact details of authorities and services available in each Member State was developed with the help of the Coordinators Group that provided the information for each country: cybersecuritymonth.eu/cyber-first-aid

There is a very big part of the EU population that does not know where to turn to in case of a cyber-incident. Sharing guidelines on what to do in case of online fraud or other cyber-security incidents would therefore add value and help achieve the campaign's objectives.

3.2 ECSM 2021 TARGET AUDIENCE PERSONAS AND RATIONALE FOR THEM

According to Europol, due to the physical restrictions enacted to halt the spread of the COVID-19, with a subsequent increase in working from home and remote access to business resources, many individuals and businesses that may not have been as active online before the crisis became a lucrative target for cyber attackers. (Source: Europol)

This leaves many groups in many categories open to cybercrime. In order to reach people with the right message in the right way, audience personas were created to better understand and communicate to those groups.

These audience personas drew on the research carried out in the PESTLE analysis which looked at the big picture across the following areas: Political, Economic, Social, Technological, Legal, and Environmental. This PESTLE analysis helped identify key audience segments and further research narrowed down the typical audience members in each segment to help develop these personas.

Heavy Social Media Users

21+ years old

Younger people are spending more time online during the pandemic due to rolling lock downs and restrictions.

Limited opportunities to socialise in person mean people are spending a lot of time connecting with friends online and are therefore vulnerable.

People Working from Home and Families

30-35+ years old

People need to use their home Wi-Fi and own devices to access confidential information from work.

They have to communicate with colleagues and their bosses digitally, through emails, and video calls, and are more exposed and vulnerable to hackers and scammers.

Women in particular are juggling work and home responsibilities including home schooling.

General Users and Online Shoppers

40-55 years old

Victims of online fraud are often individuals who are vulnerable because of their age, technical ability, and lack of awareness of fraud scams as they go about their online activities.

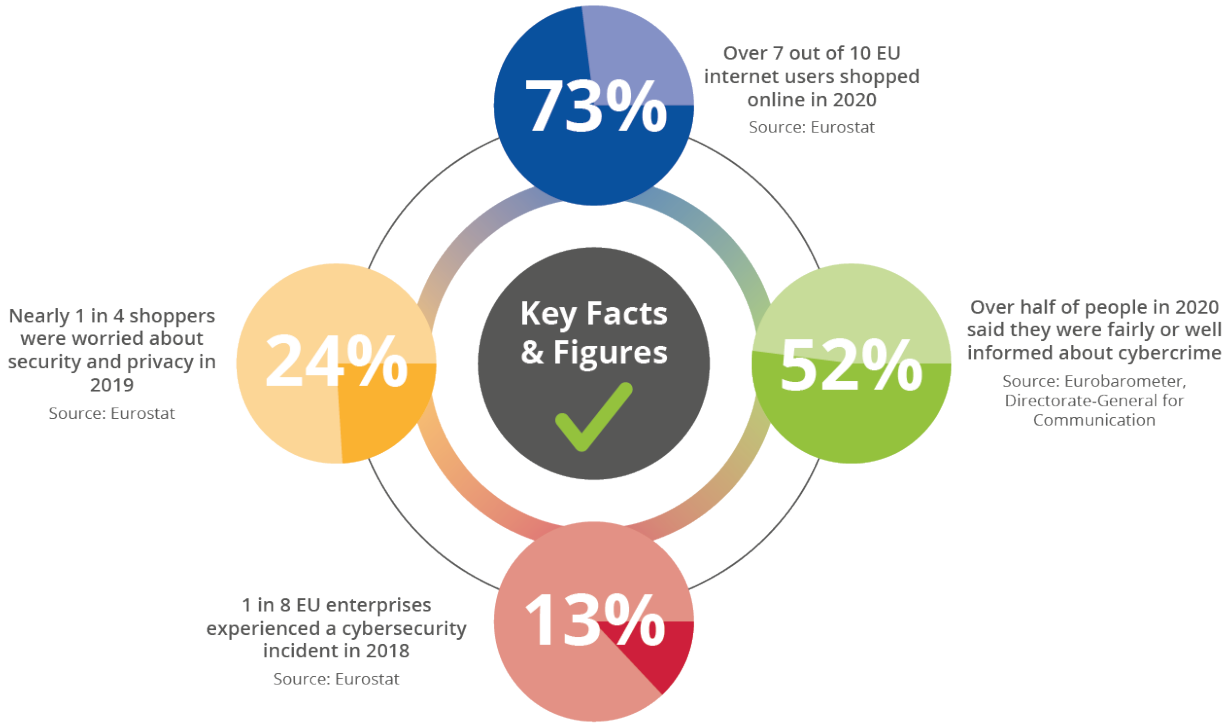
Older Users

60+ years old

Older people were forced to use online banking to pay for bills and shop by the Covid-19 restrictions. They are now using devices such as tablets regularly for the first time.

Many of them are less aware of the different types of cyberscams happening at the moment and find it difficult to spot them.

Key Facts and Figures



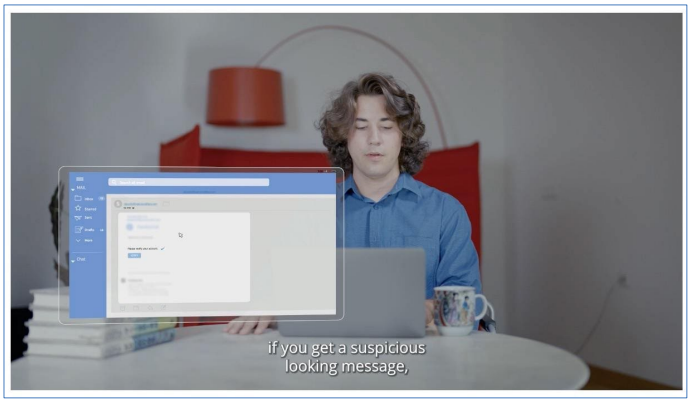
3.3 ECSM 2021 COMMUNICATIONS CHANNELS

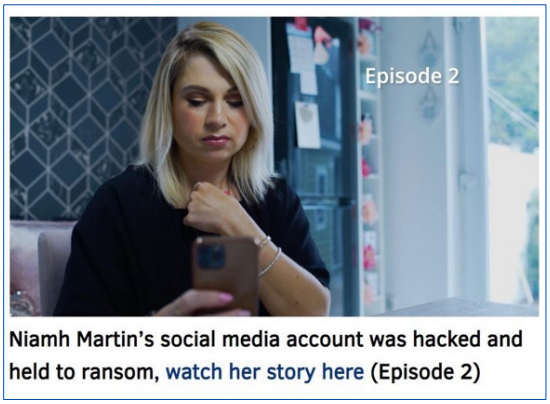
The on-going Covid-19 pandemic is leading to less of a focus on physical events and more emphasis on the online world. ECSM used a mix of social media platforms across Facebook, Twitter and YouTube in order to create an effective mix for partners to increase reach because each platform has its own distinct character and user profile. A mix of both organic and paid social media posts were used to increase reach and drive engagement.

A mix of media was created to help partners and stakeholders get the message out. The visual identity was kept consistent with previous years and emphasised the slogan "#ThinkB4UClick". This consistency is important from a "branding" point of view as ENISA grows awareness ECSM from year to year. Tailored communications toolkits were created for Ambassadors, Partners and Media. Press releases were also sent out detailing the plans for the month.

From the experience of previous years, ECSM planners knew that offering more information via website links and landing pages creates more engagement. This led ENISA to update the ECSM website cybersecuritymonth.eu with landing pages linked to themes and topics. An interactive map was added to the website to enable people across Europe to find out quickly who they should turn to for help if they were targeted by cybercriminals. News items on the web were also included to increase reach.

One of the key learnings from ECSM 2020 was that video content is an effective way to grab people's attention on social media channels. This year a series of 6 short videos were created that featured stories of real people who had been targeted by cyber attackers. These films were created to highlight the issue, to show how the person dealt with the crisis and to give advice on what to do if it happens to you.





Creating content centrally in different languages also resulted in improved workflow for the translation of material and ensured consistency across content in all languages. The videos were produced in English and subtitled with translations in the official EU languages as well as Norwegian. A parallel series of 4 creative videos were also produced to increase the reach of the campaign.

A series of 3 infographics were produced for each of the 2 themes. These were created in 23 EU languages and Norwegian (144 infographics). Short videos that could be used on social media to promote each of the infographics were also produced (144 videos).

Visual social media posts with useful tips and gamified elements, making the viewer work a little bit to earn the message also made engagement more effective. Amongst other updates, infographics were posted that offered useful and practical advice that was clear and easy to follow. People were also challenged and educated with the cybersecurity quiz.

See Annex A for a selection of the multimedia content produced along with clickable links to view them online.

4. EXECUTION PHASE

4.1 CONTENT CALENDAR

Day-by-day content calendars were developed to synchronise posting across ECSMs own channels and those of the Member States.

The first content calendar was created for the promotional campaign in June, running from 1-30 June 2021.

The main content calendars were then created to cover ECSM itself. There were different versions, one for internal ENISA use and another one for sharing with the Member States (as shown in Annex B).

The internal one was more detailed, containing extra information needed to run the campaign. This internal content calendar ran from 28 September to 31 October 2021. The content calendar for the Member States was focused on the posts and information most relevant to them and ran across a slightly narrower time period from 29 September to 29 October 2021.

The content calendars had different columns that set out information such as:

- Theme
- Date to Publish
- Creative Name
- Explanatory Notes
- Copy for Social Media Post
- Paid Post / Organic Post
- Media Spend

The content calendars worked very well as tools to enable coordination of the campaign both centrally by ENISA as well as to help synchronising posts with the Member States.

One of the challenges encountered was making sure fast-turnaround changes were shared with the Member States so that they were always using the latest version. In the future, it could be worth considering using a shared online calendar on a secure collaborative online platform so that everyone could be sure they were always looking at the latest version.

4.2 LAUNCH OF THE ECSM 2021

On September 29 an Inter-institutional launch event brought together many key players and was a great platform to begin the month's activities. The agenda and recordings are available online at this link.

Significant support was given to the launch by European Commission Vice-Presidents and other members of the College :

- Message by EC Vice-President Margrethe Vestager
- Message by EC Vice-President Margaritis Schinas
- Message by EC Commissioner Johannes Hahn
- Message by EC Director-General Mario Campolargo
- Message by the Head of CERT-EU Saad Kadhi

Margrethe Vestager, European Commission Vice-President for a Europe fit for the Digital Age and Competition presents the

Also, for the first time this year, the winning team at the European Cybersecurity Challenge became ECSM ambassadors.

4.3 CAMPAIGN MATERIALS AND SOCIAL MEDIA CONTENT

Here is an overview summary of the materials shared during the campaign. A huge amount of content was created by ENISA and the Member States, a selection of which is shown here. The revamped interactive quiz also went live during the month. More of the content is shown in the Annexes.

4.3.1 Be Cyber Secure from Home

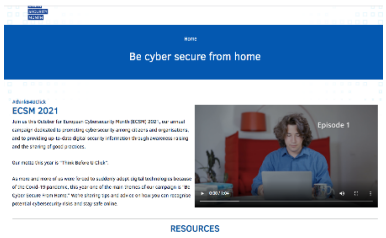
Infographic: Tips on how to keep your home safe

October 4

Video: Find out what could happen if you share private information online.

October 5

Video: He never thought it would happen to him, but one day Patrik Pallagi discovered he'd been hacked! Find out what he did next



October 6

infographic: Tips on how to help keep your accounts secure

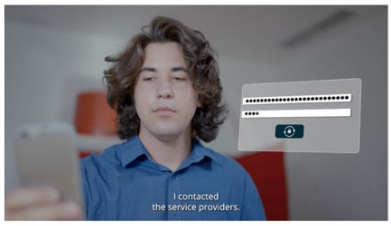
October 8

Video 2: Patrik Pallagi. What would you do if you'd been hacked?

Video: The risks if you don't keep your digital devices updated

October 12

Infographic: Advice on how to protect yourself as you connect, share and communicate online

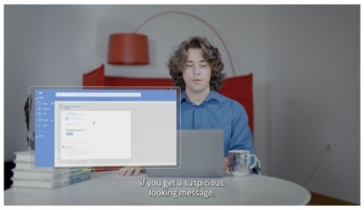


Patrik Pallagi never thought it would happen to him, but one day he realised he'd been hacked. Watch his true story here (Episode 2)

October 11

Video 3: Patrik Pallagi. Find out what he learned from his experience

October 13



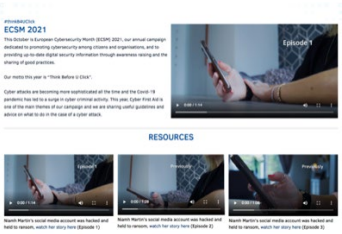
October 14

4.3.2 Cyber First Aid

Interactive Map to find local services you can contact if you are the target of online shopping fraud or social media account hack.

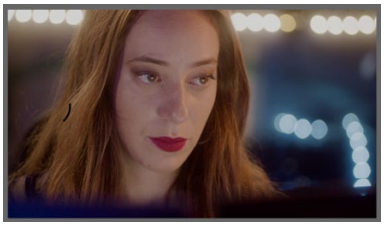
October 15

ECSM Quiz. Test your cybersecurity skills.



October 18

Twitter: **Ask the Experts** session.

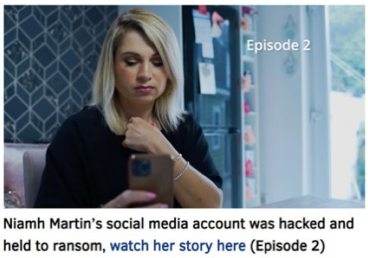


October 19

Video 1: Niamh Martin's social media account was hacked and held to ransom

October 20

Video: Find out more about how you know you can, and should, report cybersecurity attacks.



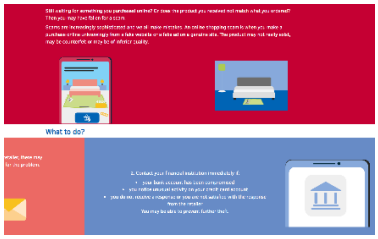
October 22

Infographic: Tips and advice How to know if your social media account has been hacked and what to do about it.

October 25

Video 2: Niamh Martin. Her business was almost destroyed by hackers.

Infographic: Tips and advice on what to do if you saw unusual activity on your credit card or bank account.



October 26

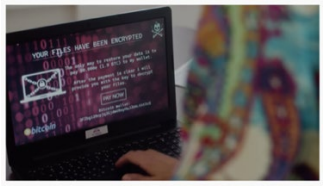
Video 3: Niamh Martin shares what she learned after her business survived a ransomware attack.

October 27

Podcast: CYBERSNACS interview with ENISA's Demosthenes Ikonomou

October 28

Infographic: Advice on what to do when shopping online.



October 29

4.4 CAMPAIGN STORIES

The stories of the campaigns rolled out in the Member States are inspirational and instructive. We present here a small selection as a representative sample. Collecting these stories enables the sharing of best practice between Member States and the wealth of material provided this year demonstrates exciting opportunities for fostering this collaboration and sharing in future years.

Czech Republic

It is also important to complete the posts with eye-catching pictures. Especially children attach great importance to the visual side. It is our message and challenge for next year´s campaign too.

https://www.instagram.com/p/CVKGr8-oiGJ/

Malta

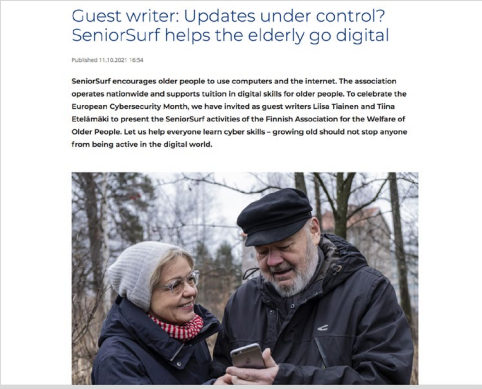
Exposure has been given to Cyber Security Malta on various platforms, namely, TV, radio, online portals, and traditional newspaper as well as on social media. Given the reach and query for assistance received, awareness was well engaged with the general public and there is the desire for more information.

Bulgaria

As long as there is a continuously on-going discussion of cybersecurity risks and awareness, at some point the audiences we targeted will adopt cybersecurity advice as an essential part of their online presence and behaviour.

Finland

The best thing about ECSM campaign is that it brings more materials - tips and advice for every day cyber life - to our website. Those materials (along with the guidance produced by NCSC-FI) can be shared by our ministry, other state offices and other organisations we work close with.

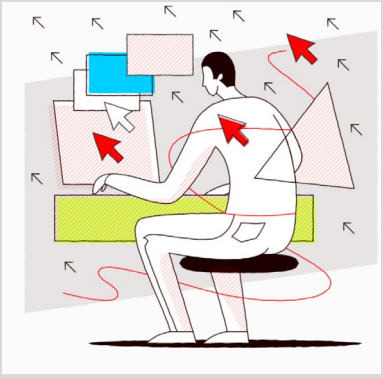

Guest writer: Updates under control? SeniorSurf helps the elderly go digital

Published 11.10.2021 16:54

SeniorSurf encourages older people to use computers and the internet. The association operates nationwide and supports tuition in digital skills for older people. To celebrate the European Cybersecurity Month, we have invited as guest writers Liisa Tiainen and Tiina Etelämäki to present the SeniorSurf activities of the Finnish Association for the Welfare of Older People. Let us help everyone learn cyber skills – growing old should not stop anyone from being active in the digital world.

Luxembourg

The fact that the ECSM has now a fully-fledged campaign is certainly an advantage to better reach the user with a coordinated European message. Cybersecurity is a shared responsibility and at national level we will continue to support the ECSM.
https://www.cybersecurityweek.lu/



Slovakia

The majority of cyber attacks are still a result of human error, which is why we believe that the best protection or “antivirus” is knowledge. By offering this free course, we are giving each user the opportunity to educate themselves on cybersecurity and obtain the necessary knowledge and skills to stay secure in the workplace.

5. EVALUATION

5.1 FOCUS OF MEASUREMENT

Overall, there were effectively three ways in which data was collected: One source was data gathered centrally which is directly - for example about social media paid posts; Local data was collected from member states via a questionnaire; and data from “earned channels”, such as the chatter on social media, which was collected using a third party social media listening tool that listens to conversations “in the wild” (shown here).

The goal was to move towards real world impact and how that might be measured. To that end proxy measurements were sought for behavioural change, which is challenging to measure in itself. However, some assumptions can be made to extrapolate the information from those elements that can be measured. For example, it is possible to determine how much of a video that was posted was watched by a viewer. If the person was interested enough to watch the video, then it can be assumed that they are engaged. That means engagement can be used as a proxy for interest and interest as proxy for behavioural change.

5.2 QUESTIONNAIRE OPTIMISATION

In order to precisely evaluate and assess the effectiveness of ECSM it is crucial to have good data from Member States. The objective this year was to increase the Member States’ response rates for the evaluation questionnaires and to gather better quality data using scientifically validated metrics. To this end extensive work was done by the task force in improving the questionnaire. This resulted in 26 countries filling in the evaluation questionnaire this year compared to 19 in 2020.

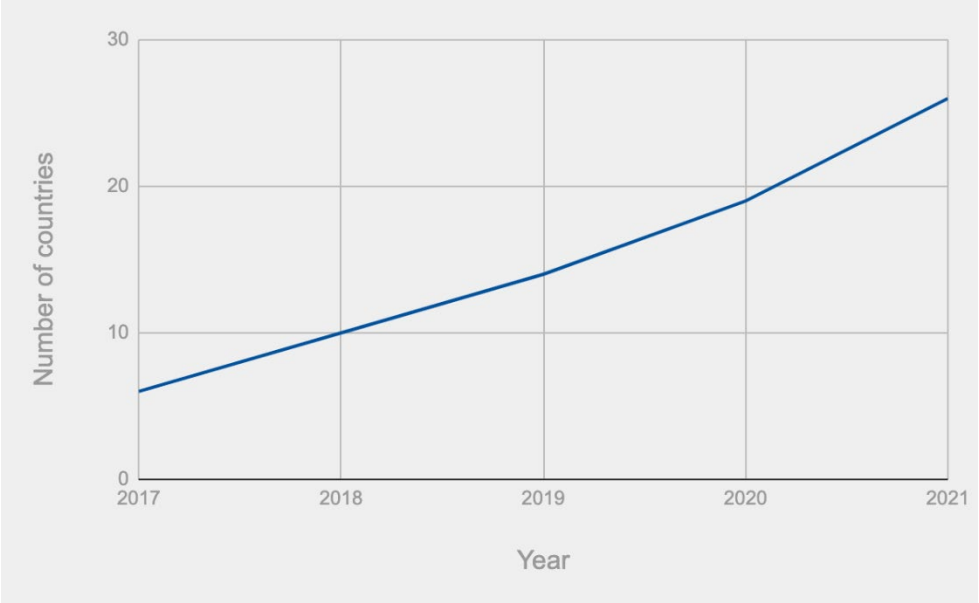
The questions were scrutinised by the task force to make them more targeted, useful and relevant. The data type of each field was properly ordered into qualitative, quantitative, open text and Likert values. Specific fields were made mandatory to avoid empty fields for crucial information.

This year it was decided to include not only the questionnaire itself but also an analytics spreadsheet (with questions such as those shown here) as well as a story template document to enable ENISA to have more qualitative and quantitative data for the ECSM. This gave Member States a more structured and flexible way to share their activities and their outcomes as well as to collect the appropriate data internally.

1	Web Analytics
2	**Questions**
3	Country Name
4	Do you have a specific website for the ECSM campaign?
5	If not, do you plan to have a specific website for ECSM within 3 years?
6	Do you have specific landing pages for the ECSM campaign?
7	Has there been an increase, decrease or no change in the number of people who visited the website in October 2021 i comparison to September 2021?
8	What is the percentage of the increase or decrease in website visitors during October 2021 in comparison to Septembe
9	What is the percentage of the increase or decrease in website visitors during October 2021 in comparison to October 2
10	What is the percentage of visitors to the website who entered and then left without clicking to anywhere else on your
11	What is the number of unique visitors of your ECSM website in October 2021?
12	What is the total number of visitor actions (e.g. page views, registrations, form submissions) that occurred on the web
13	What is the average time the webpages were viewed by visitors in October 2021?
14	What is the average time visitors actually interacted during the page viewing in October 2021?

Details of the number of Member States and other countries who took part in the evaluation by returning at least the EUSurvey Questionnaire are presented in the table below.[1] This year, this figure was up by 7 to 26 countries from the figure of 19 in 2020. This increase of 37% is largely due to the deeply collaborative approach taken to the questionnaire design this year.

More countries are participating in the evaluation every year



5.3 ASSESSMENT OF IMPLEMENTED ACTIONS BASED ON THE EVALUATION METHODOLOGY

In this section we present the results reported by the Member States in their survey responses. The qualitative data responses were studied to identify themes and representative samples are included here. All feedback received has been reviewed and follow up actions taken into consideration.

5.3.1 Results of Member state EUSurvey Questionnaire

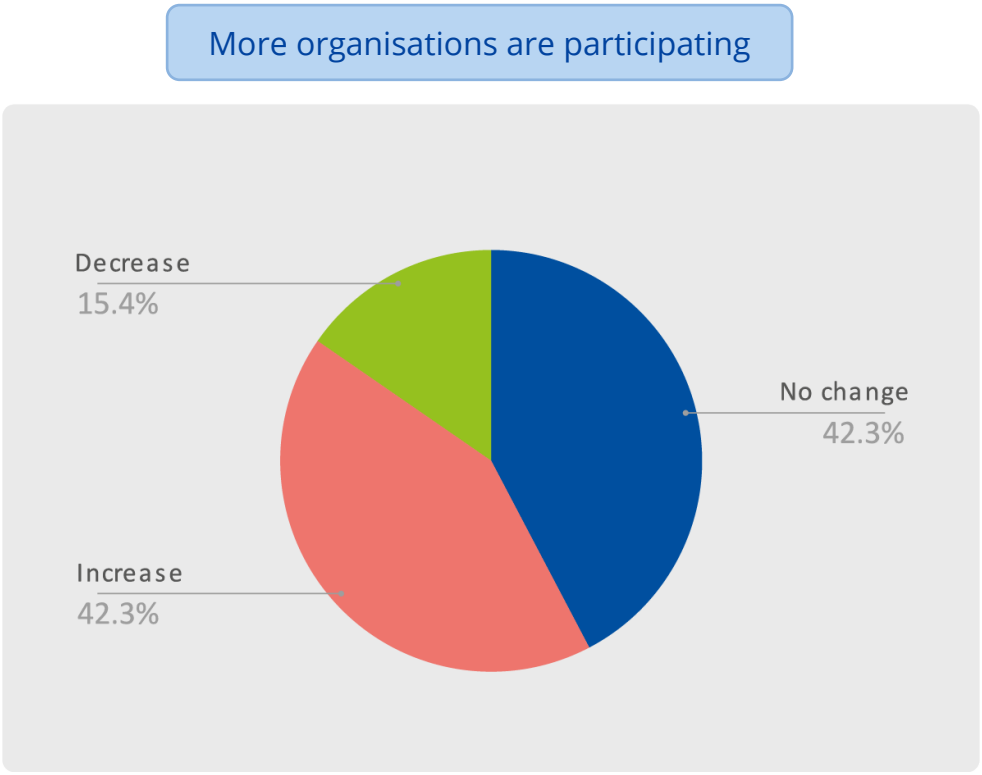
5.3.1.1 Campaigns

In relation to the Member State campaigns, **over two thirds of respondents (69%) said they had organised specific ECSM campaigns**.

There is a big variation in the number of organisations (for example, number of schools etc.) that participate in ECSM from country to country. Some reported as many as 100-2,000 organisations taking part although the median figure was approximately 22 because the figures were much lower in some countries.

[1] *The campaign in Belgium ran on different dates to the main ECSM campaign in October, and provisional figures were provided by them in their questionnaire responses at the time of writing.*

Overall, more organisations in the Member States participated this year than previously as shown in the chart below:



The average growth in the number of participating organisations year-on-year was **an increase of 46%.**

The most common types of organisations that took part were **Public, Private and Education** although several countries also mentioned that **NGOs** had taken part in their campaigns.

In terms of resourcing, on average **46 person days** were allocated by each Member State coordinating organisation to ECSM 2021. This is up significantly from the 31 person days of 2020.

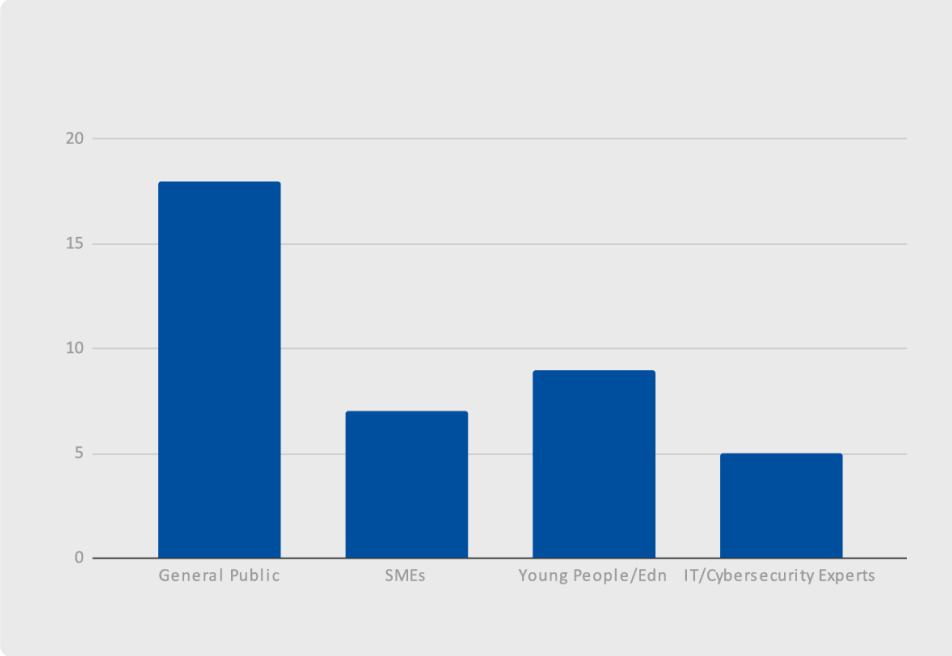
A third of organisers had **2 or more full time employees fully focused on ECSM**, a third had one person full time on ECSM, and the remaining third had no full-time people focussed exclusively on ECSM 2021.

The most common departments these people worked in were **Communications and IT**, although interestingly **Cybersecurity and HR** teams were also involved in some Member States.

The cost of ECSM activities varied greatly, with **just over half (54%) reporting no costs**. Of those with costs for ECSM activities, the **average cost was €79k per Member State**.

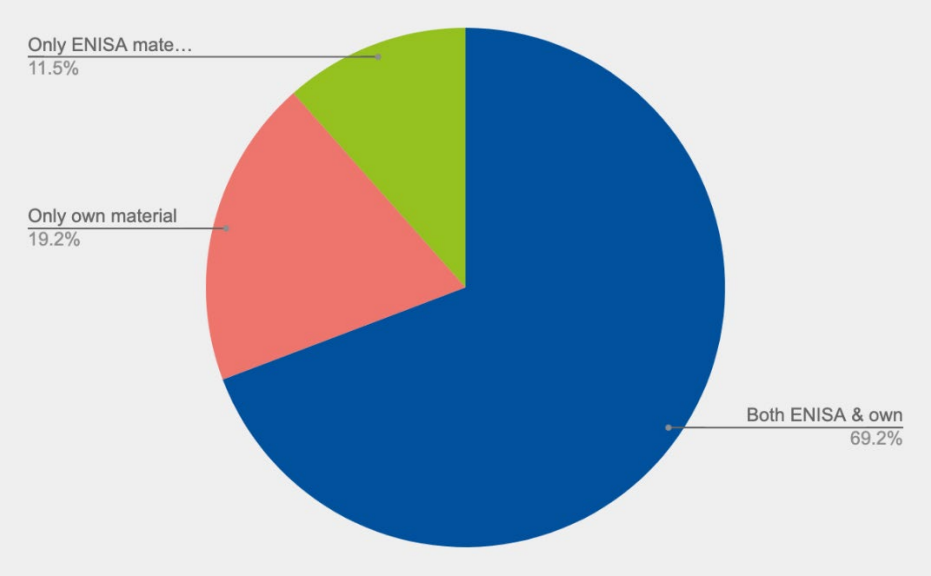
The target audiences in each Member State spanned a wide range. Notably, **young people** were a focus for many countries as well as **cybersecurity experts**. This indicates an interest in **reaching "middlemen" experts** who work in the area of cybersecurity.

The audiences range from the public to experts



As would be expected, the average duration of the ECSM campaign was also **5 weeks** in the Member States reflecting the focus on the month of October itself. In a sign of how useful the Member States find the ENISA-generated content, **most Member States used ENISA material** either exclusively or in conjunction with their own materials:

Most countries used ENISA materials



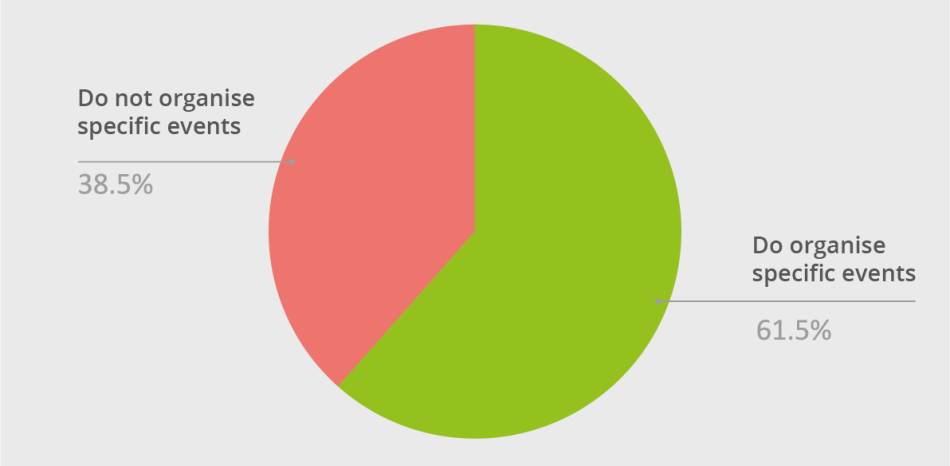
The average number of security themes or topics covered varied greatly, and on average 12 themes were covered in each country, but many preferred to **focus on 3 core themes/topics**.

In addition to the two overall themes of the ECSM campaign, Member States also focused on a wide range of other themes from **election security** to **women in cybersecurity**. The themes and topics captured in the survey give a rich source of inspiration for future editions of ECSM.

5.3.1.2 Events

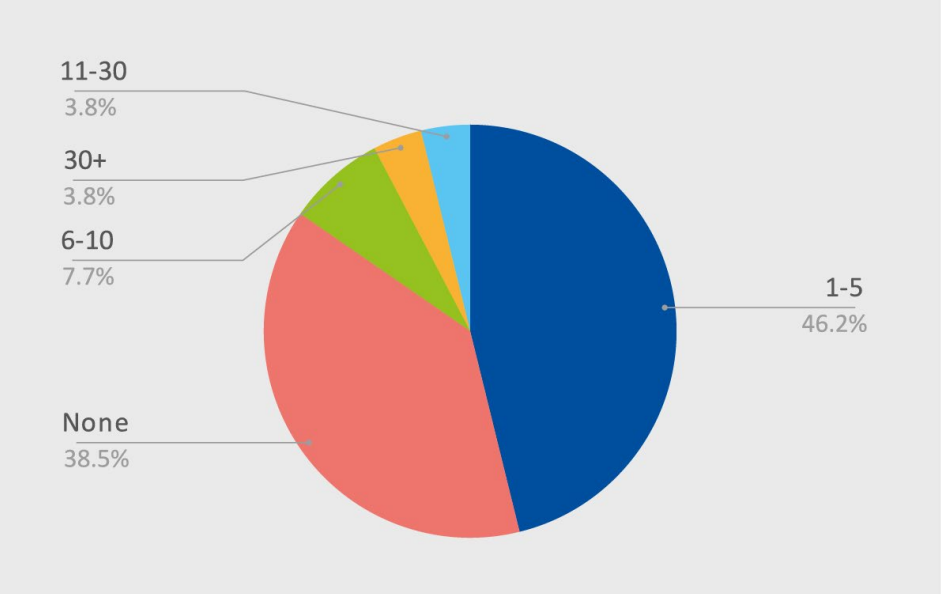
Nearly two-thirds (62%) of Member States organised specific events for ECSM 2021 (either online or in person):

Most organise specific events for ECSM (online and face-to-face)



Many of these conferences/workshops catered for **more than 50 attendees**. Some countries organised 1 such event while others organised **up up to 30 events**:

Many conferences/workshops with over 50 people were organised



Although many events were small scale with approximately 50 attendees, **several attracted over 500 attendees** possibly due to their hybrid and/or online nature during the pandemic. It was these larger events that had significant budgets associated with them.

Among the most popular materials and content distributed were **videos, articles and podcasts**. Interestingly, several Member States also organised **live streamed social media events**, while one country shared a **free online eLearning course** and others shared **guidance documents**. This provides valuable inspiration for future ECSM content.

Most Member States (nearly 70%) don't collect feedback from attendees in a structured way yet.

However, almost all Member States believe strongly that attendees **would recommend these events** to their family and friends.

5.3.1.3 Feedback

Just under half of respondents (46%) obtain feedback from users in relation to their campaigns. This shows the opportunity for improving best practice for the future by obtaining more feedback and creating more appropriate campaigns in response to user feedback.

The main **strengths** highlighted in the feedback received from users included:

- *Practical tips such as infographics working well*
- *Themes were of interest to the public*
- *Powerful messages resonated*

Some **weaknesses** mentioned in the feedback included:

- *Too many events to attend online, missing 'physical' events during the pandemic*
- *Knowledge and awareness are a prerequisite to change behaviour but not necessarily sufficient*
- *The need for more awareness materials for non-expert users*

Similarly, **46% of Member States obtain feedback from partners** about ECSM.

Some of the **strengths** highlighted in the partner feedback received included:

- *The materials used (videos & infographics) were very useful and interesting*
- *Great materials for distribution*
- *Inspiration and energy*

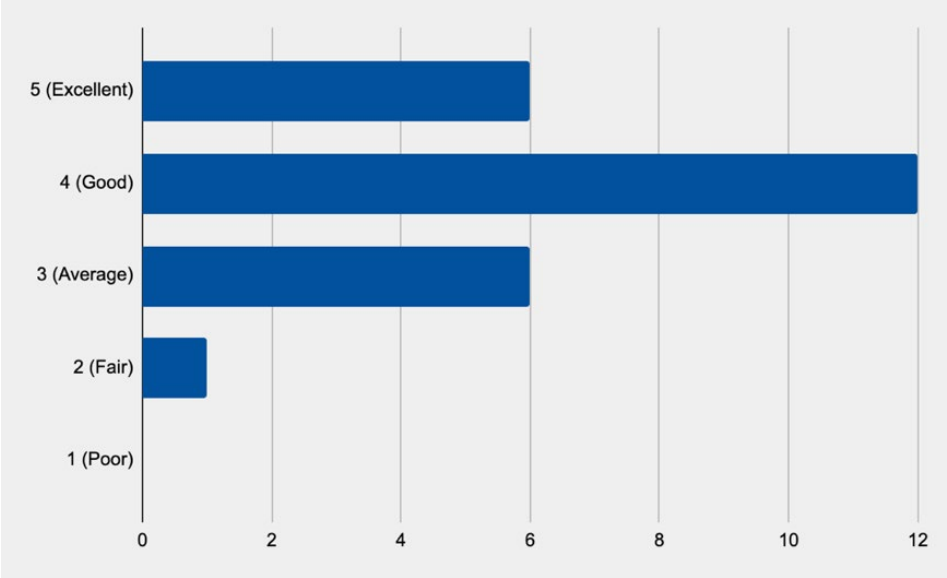
Several **weaknesses** partners mentioned in their feedback were:

- *The need for more content for young people*
- *Lack of funding for advertising on social media*
- *The absence of physical events*

Some Member States had suggestions on how ENISA could continue and increase support to help them deliver more effective campaigns. Among the representative comments and suggestions coming through in this feedback were:

- *"I think ENISA works very well on the campaigns. Of course, there are always things that can be improved, but overall, I am very happy with the way it works."*
- *"Support is good as it is."*
- *"Determining the topics earlier, so our campaigns can be aligned."*
- *"You are doing a great job through the year. It is difficult so balance a one size fits all campaign, but your work serves as an inspiration for our national campaign activities."*

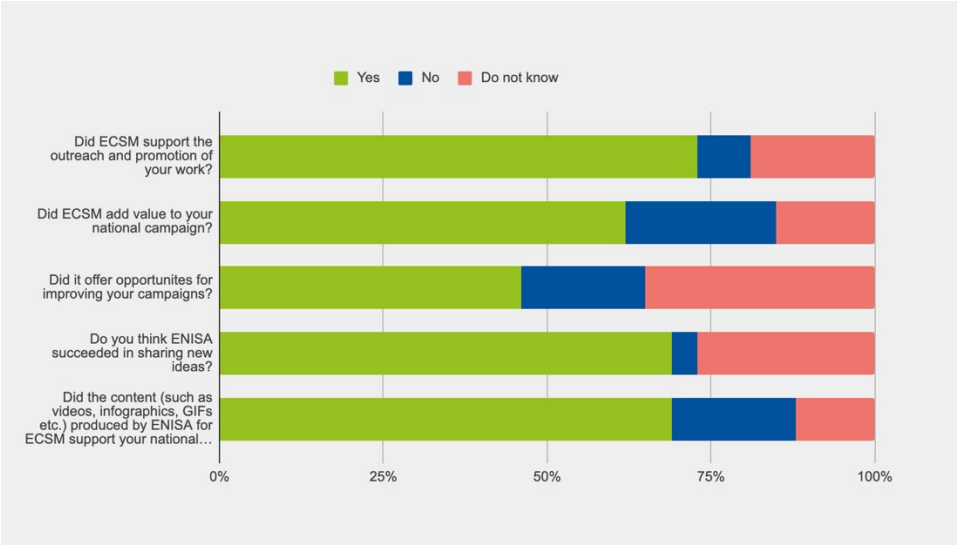
Over two thirds of Member States who responded (69%) rated the overall implementation of the ECSM2021 campaign as **Good or Excellent** (similar to the previous year's figure of 78%):



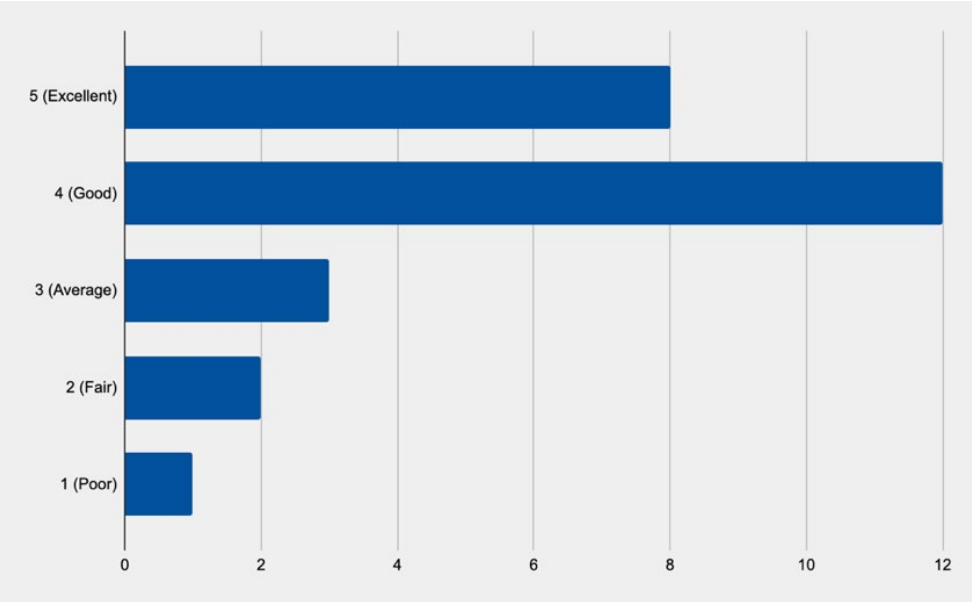
Among responding Member States:

- 73% believed ECSM2021 supported their outreach and promotion work (19% did not know, 8% disagreed)
- 62% said ECSM adds value to their national campaign (23% felt it did not and 15% did not know)
- 46% believed ECSM did offer opportunities for improving their national campaigns through international collaboration (35% did not know, and 19% felt it did not)
- 69% said ENISA succeeded in sharing and promoting new ideas among ECSM partners (4% said it had not, and 27% did not know)
- 69% reported that the content such as videos, infographics, and GIFs produced by ENISA for ECSM supported their national campaign (19% did not report that and 12% did not express an opinion)

Most MS believe ECSM supports their national campaigns



The **content** produced for the ECSM2021 campaign was rated as **Good to Excellent by 77% of Member States**:

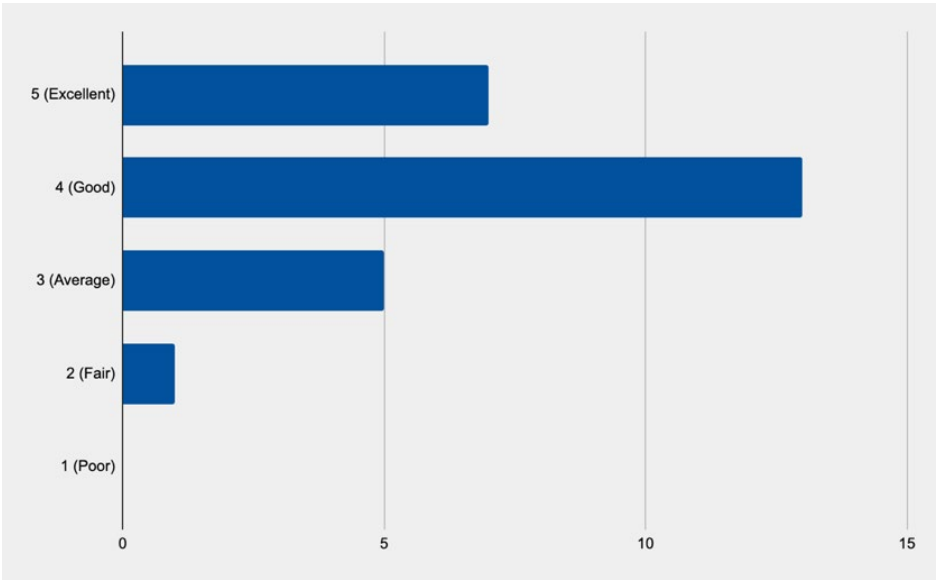


Looking to the future, some Member States had suggestions for materials or content ENISA could offer to support their campaigns. This included:

- eLearning courses
- material aimed more at young people
- more videos with real experiences

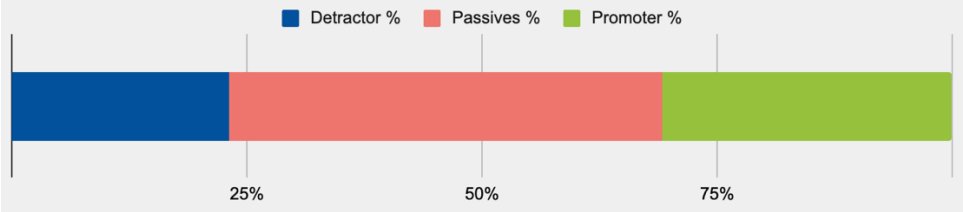
Only 39% believed ENISA could promote their awareness material better, and 69% believed that ECSM offers opportunities for fostering a pan-European cybersecurity culture.

A significant majority of 77% rate the implementation of the ECSM2021 campaign by ENISA **Good to Excellent**:

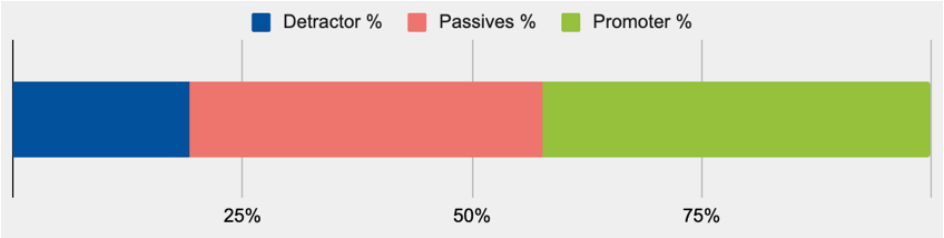


Member States were also asked how they would recommend the support received from ENISA in relation to ECSM on a scale of 1 to 10 (where 1 is low and 10 is high). This follows a Net Promoter Score (NPS) approach which divides respondents into "promoters" who provide ratings of 9 or 10, "passives" who provide ratings of 7 or 8, and "detractors"

who provide ratings of 6 or lower. The resulting NPS is then calculated by subtracting the proportion of detractors from the proportion of promoters. [2] More Member States would recommend ENISA's support than otherwise as shown by the calculated **positive Net Promoter Score (NPS)** figure of 8 and the stacked bar chart below:



This Net Promoter Score is a particularly useful metric because it identifies areas where attention should be directed and where appropriate actions or interventions implemented. A similar methodology was used in a related question about whether the MS would recommend partnering with ENISA on ECSM next year to another organisation like theirs. Significantly more MS would recommend this partnership than not, and the resulting **Net Promoter Score (NPS) was very positive at 23**. This shows how valuable the partnership with ENISA on ECSM is perceived by the MS. This is represented visually below:



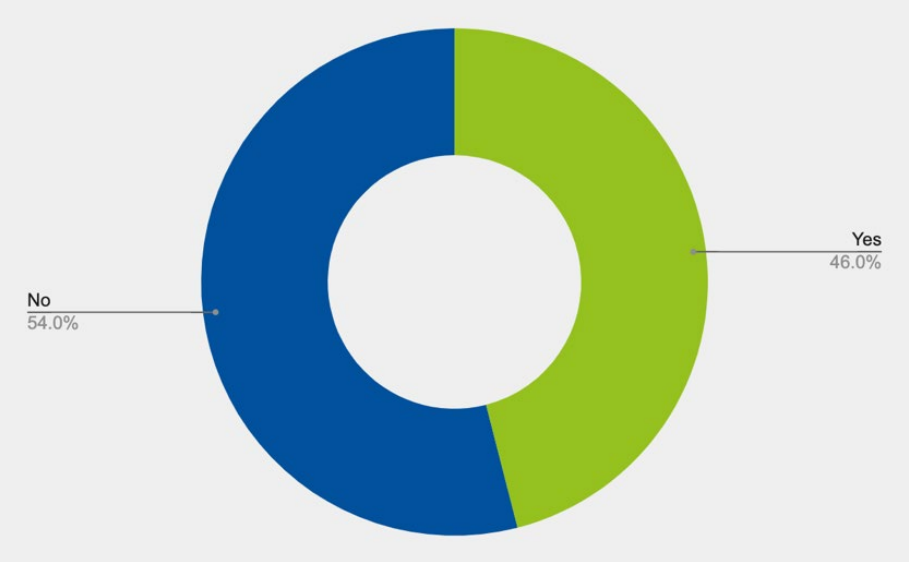
5.3.1.4 Measuring Behavioural Change

The intention this year in relation to measuring behavioural change was to collect data from Member States to better understand how effective they perceive their campaigns to be in facilitating behaviour change, and to develop strategies that work to drive behaviour change that is conducive to cybersecurity, rather than simply educate and inform target audiences. By involving and inspiring the Member States to consider end user behaviour as part of the design of the campaigns, rather than simply providing information to stakeholders through a variety of channels, they are significantly improving the impact of their campaigns. A full concept was developed to provide a framework on which behavioural research can commence by working in partnership with MS.

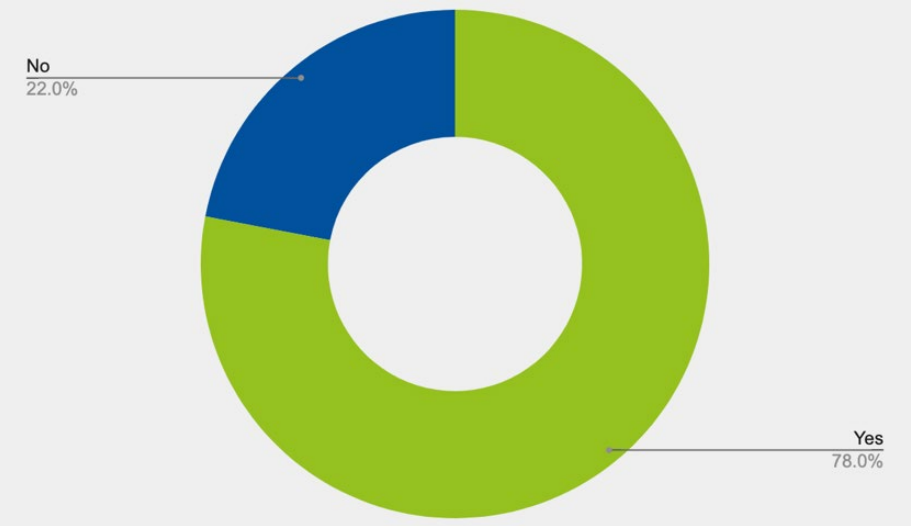
Although the questionnaire results show there was relatively low confidence in being able to measure behaviour change with specific users among MS, in fact **46% of them were able to obtain the required data** for the measurement of behaviour change (such as number of people signing up for training, or the percentage of people reporting a potential phishing email). This suggests there may be an opportunity to educate and inform MS as to how behaviour change can be measured more in the future.

[2] Source: "Net promoter score," Wikipedia https://en.wikipedia.org/wiki/Net_promoter_score

Nearly half of MS can obtain behaviour change metrics

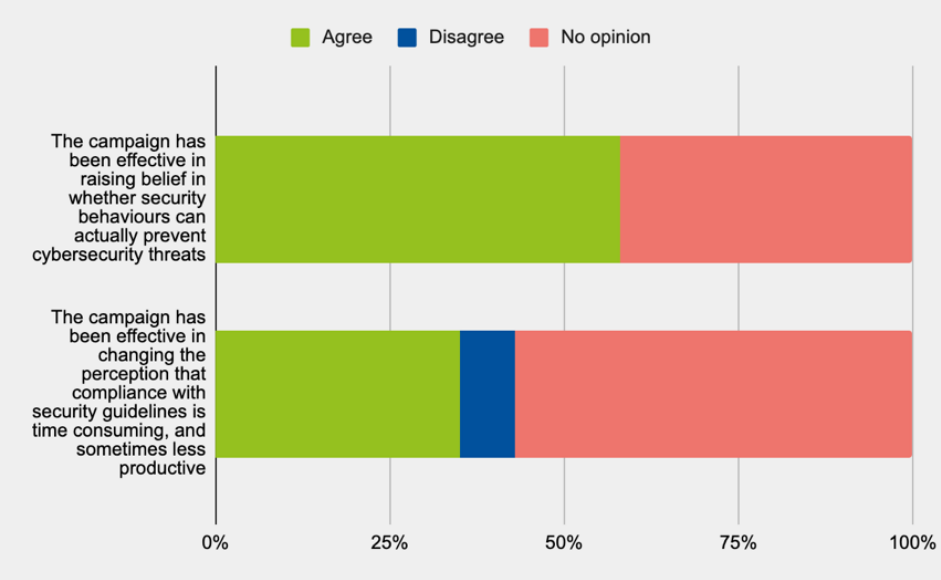


Looking at ways to overcome the challenges involved, two key points emerged from the feedback: **surveys** were seen as the most feasible way of measuring behavioural change, and the fact that it was a "**difficult**" task in general to do was mentioned repeatedly. Quizzes or other knowledge assessment approaches were **run by 35%** to assess the knowledge of citizens or users as part of ECSM. Of those who do run these, **78% have seen an increase in performance** of the participants at the ECSM test/quiz as a result of the campaigns:



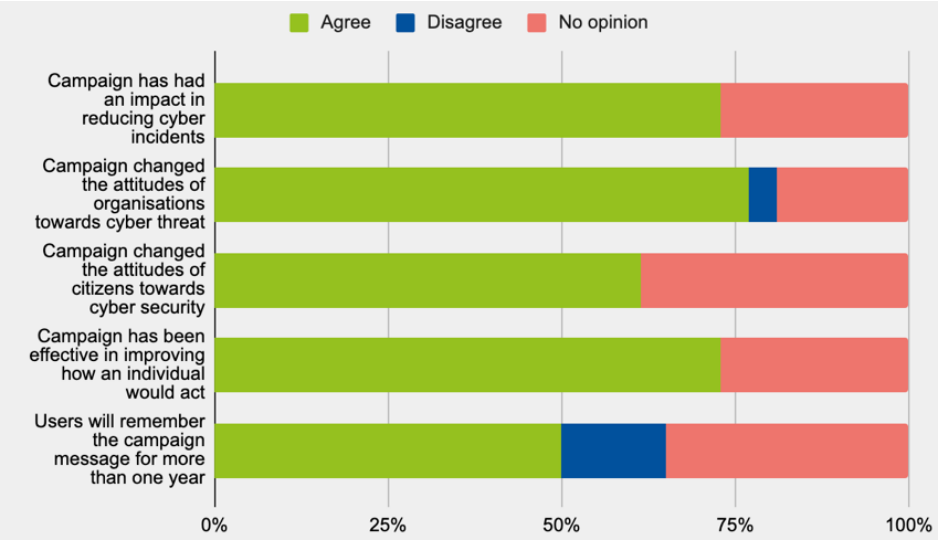
Just over half of MS (58%) agreed or strongly agreed with the statement that the campaign has been effective in raising belief in whether security behaviours can actually prevent cybersecurity threats. But only 35% agreed that the campaign has been effective in changing the perception that compliance with security guidelines is time consuming, and sometimes less productive, perhaps reflecting the technical challenges end users face in following best practices.

Campaigns are seen as being effective although challenges remain



Looking at the impact of Member State campaigns as reported in the survey responses also yields valuable insights:

- **73% agree** that their campaign (or their partners') has had an **impact in reducing cyber incidents** (with the remaining 27% expressing no opinion)
- **77% agree** that their campaign (or their partners') has **changed the attitudes of organisations** towards cyber threats (only 4% disagreed and 19% had no opinion)
- A slightly lower figure of **62% agree that they've changed the attitudes of citizens** towards cybersecurity (with 39% having no opinion and none disagreeing)
- **73% say that their campaign has been effective in improving how an individual would act**, if they are faced with a cybersecurity threat (the remaining 27% had no opinion on this)
- **Half of MS (50%) agree that users will remember the message** of the campaign materials for more than one year – indicating the need for ECSM every year (15% disagreed and 35% had no opinion)



Campaigns alone, particularly without user-level data, are limited in their ability to drive behaviour change when key challenges exist at a broader level. Behavioural research is therefore critical to understanding what those challenges are, particularly within organisations, with efforts made to reduce their effect to get maximum impact from awareness campaigns that are designed to reduce cybersecurity threat through user behaviour.

When asked to describe their confidence in the campaigns in delivering behaviour change at citizen level, some interesting points emerged in the comments. A representative sample are shown here:

- *"I think the campaigns were well developed so they become effective"*
- *"High Confidence in ECSM Campaign in delivering behaviour change at Citizen level"*
- *"One campaign per year is not going to change behaviour. Regular work is needed"*
- *"Awareness is key for changing use behaviour."*

5.3.1.5 Monitoring the Media in Member States

When it comes to monitoring the media (online newspapers and publications), 62% of Member States are doing that using tools such CISION, Gopress and Meltwater.

The vast majority of Member States (85%) issue press releases to the media. The 62% that have media monitoring tools in place are then also able to monitor the press release take up and results in the media.

5.3.1.6 Paid Advertising

Most Member States (73%) did not organise TV/Radio advertisement activities for ECSM 2021.

Of those who did, the ECSM advertisements were displayed typically 30+ times.

Many Member States opted for paid advertising on social media. Among them, the average spend on digital advertising on social media across all MS (and partner) campaigns related to ECSM was **€13k per MS** on paid social media advertising.

Although just over half of MS reported no change in digital advertising budget this year (54%), there were others (39%) who reported an increase.

Belief in the effectiveness of this advertising is relatively strong with just under **70% rating it as somewhat to very effective**, with only approximately 30% rating it as not effective.

5.3.2 Results of Member State Web Activities

For the first time this year, and in response to MS feedback, the analytics for web and social media activities were collected in a separate spreadsheet to the main survey. However, from the variations in the amount of data filled in it is clear that this information is still hard to collect. This is possibly due to the fact that different teams look after web and social media in the MS organisations. The different analytics platforms being deployed on their websites would also lead to variations in data availability.

This makes cross country comparisons difficult, but some general comments can be made:

- Only 3 countries report having dedicated ECSM websites
- However, an additional 4 countries have landing pages specific to ECSM
- Most MS report an increase in visitors to their websites and landing pages in 2021

5.3.3 Results of Member State Social Media Activities

Similarly, to the website data, the social media analytics were collected in separate spreadsheet form this year. Although the data is quite detailed it is difficult to compare like with like because of the apparent variations in how the data is being collected and reported across the different platforms.

Some of the cross-cutting findings from analysis of the Member State social media activities include:

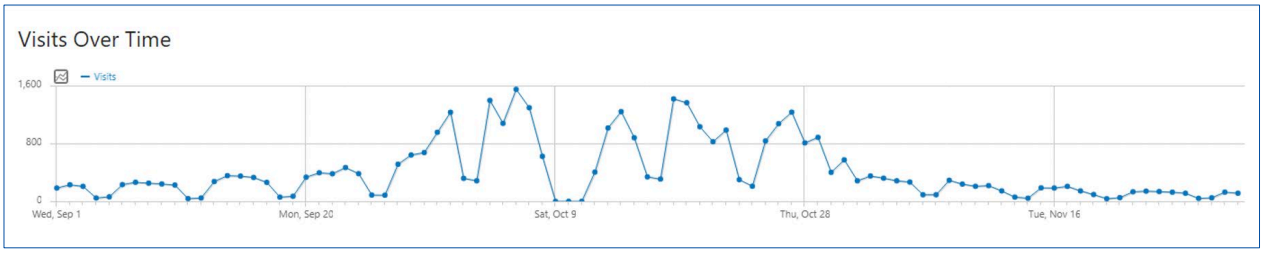
- **Local language hashtags** were used in addition to the main ECSM ones by some (for example, #Cybermois in France)
- **Different countries used different platforms for different audiences**, with many preferring to use Facebook and Instagram instead of Twitter and LinkedIn. This was most likely because this enabled them to target bigger "general public" audiences on Facebook and younger people on Instagram (pointing to a possible opportunity for evolving the ECSM social media channels in the future).
- **TikTok was used by at least one country** although data on its effectiveness was not readily available

5.4 ASSESSMENT OF WEB RESULTS

This year's centralised ENISA web analytics give a useful insight into the impact and visibility of the campaign.

5.4.1 Assessment of ECSM Website Results

A detailed analysis was carried out of the web analytics for the ECSM website during the period from 1 September to 30 November 2021. These visits over time are shown in this screenshot from the Matomo web analytics platform:

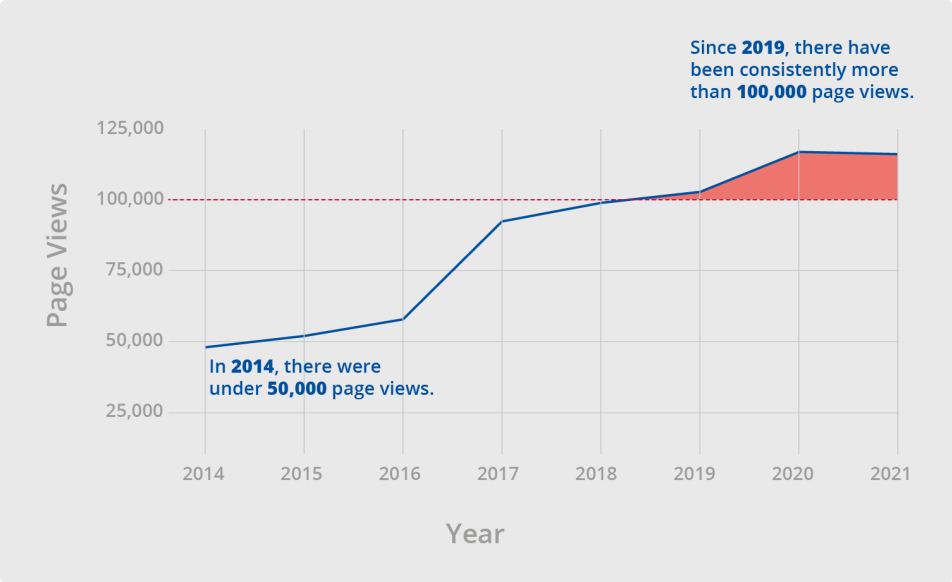


Analysis shows that:

- page views are now consistently above 100,000 views with 116,277 in 2021 (similar to the 2020 figure of 117,072 in 2020 and well up on the 102,945 of 2019)
- website visits are also consistently high with 36,051 in 2021 (up from 35, 445 in 2020 and 30,807 in 2019)
- people are spending a significant amount of time on the site with an average visit duration of 5 min 28s
- this interest is also reflected in the number of unique downloads which was 2,148
- during their visit, people carry out an average of 3.4 actions per visit (these are page views, downloads, out links and/or internal site searches)
- the graph of visits shows a weekly periodicity, with weekdays Mon-Friday being the most visited days compared to weekends
- in another improvement on previous years, the level of visits was sustained at a high level each week of the campaign in October, instead of just one big spike at the beginning of the month

The figure below shows the number of page views that the ECSM website has had from 2014 to 2021. It demonstrates that page views on the ECSM website have been sustained at over 100,000 page views since 2019. This is over twice the number of page views of the campaign in 2014.

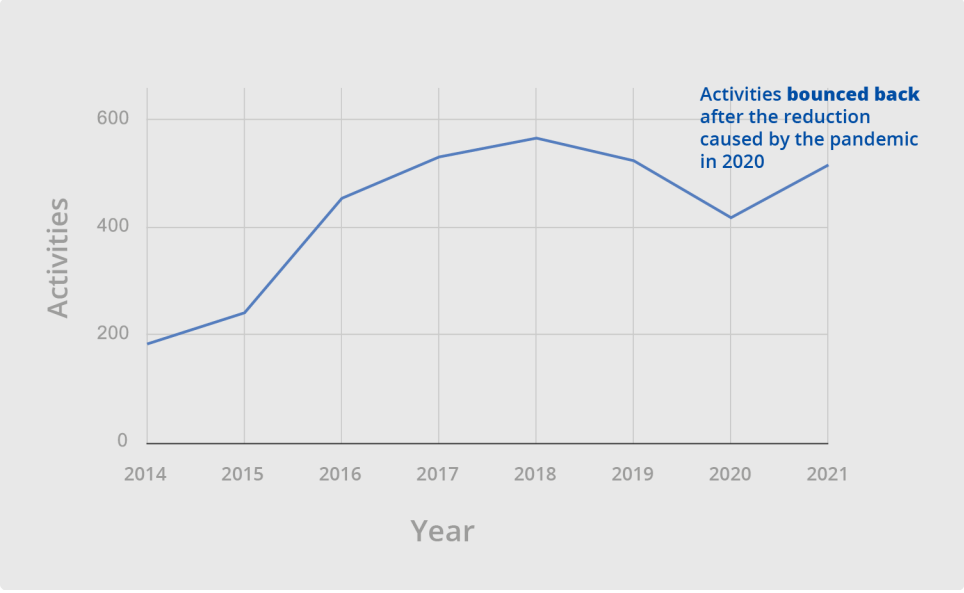
Page views are now twice what they were



5.4.2 ECSM Map of Activities

There were 517 activities registered and approved on the ECSM website for 2021. This shows an increase on the previous year, presumably as organisers got used to the “new normal” of the pandemic and again started organising more online, hybrid and physical events. The number of countries organising events (29) was approximately the same as last year which shows that more activities were happening in each country. The figure below shows the total number of events that took place in October 2021 compared to previous years showing the “bounce back” effect:

Activities increased significantly this year

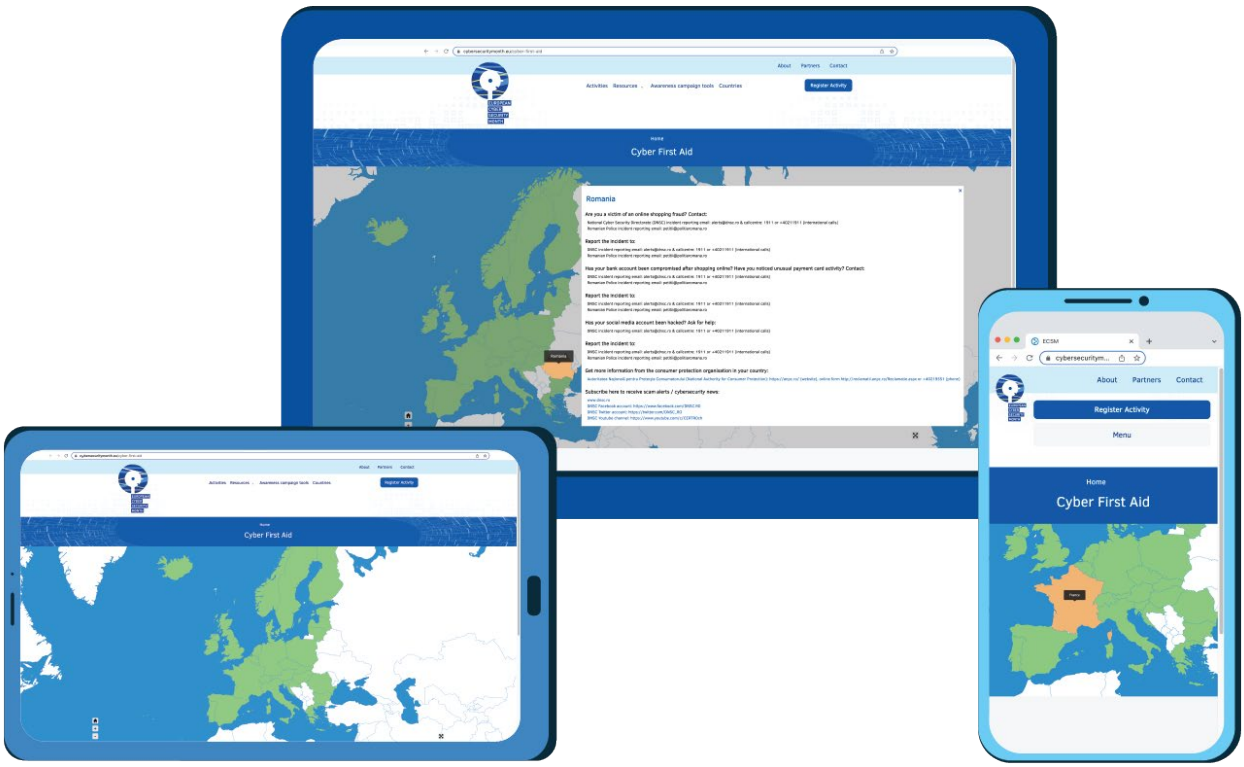


5.4.3 ECSM Interactive Map

For the first time this year, an interactive map was created to point people to in-country resources they could go to if they had been targeted by cyber criminals and needed help. This was important because clear contact information and pathways enables better reporting and protection against cybersecurity threat.

For this reason, an EU map with contact details of authorities and services available in each Member State was developed with the help of the Coordinators Group that provided the information for each country. This was challenging to create as the approach in each Member State to cyber crime varies greatly. The resulting interactive "Cyber First Aid" map is now a valuable online resource that will be updated regularly as shown in this screenshot.

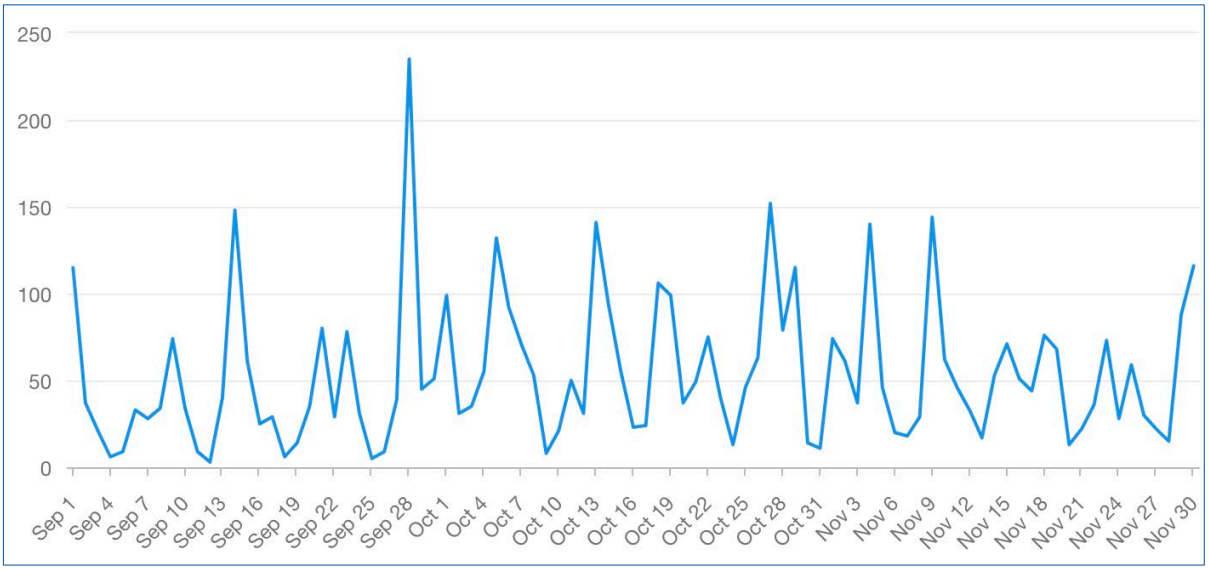
The ECSM Interactive Map can be accessed online at the following link: https://cybersecuritymonth.eu/cyber-first-aid



5.5 ASSESSMENT OF MEDIA MONITORING RESULTS

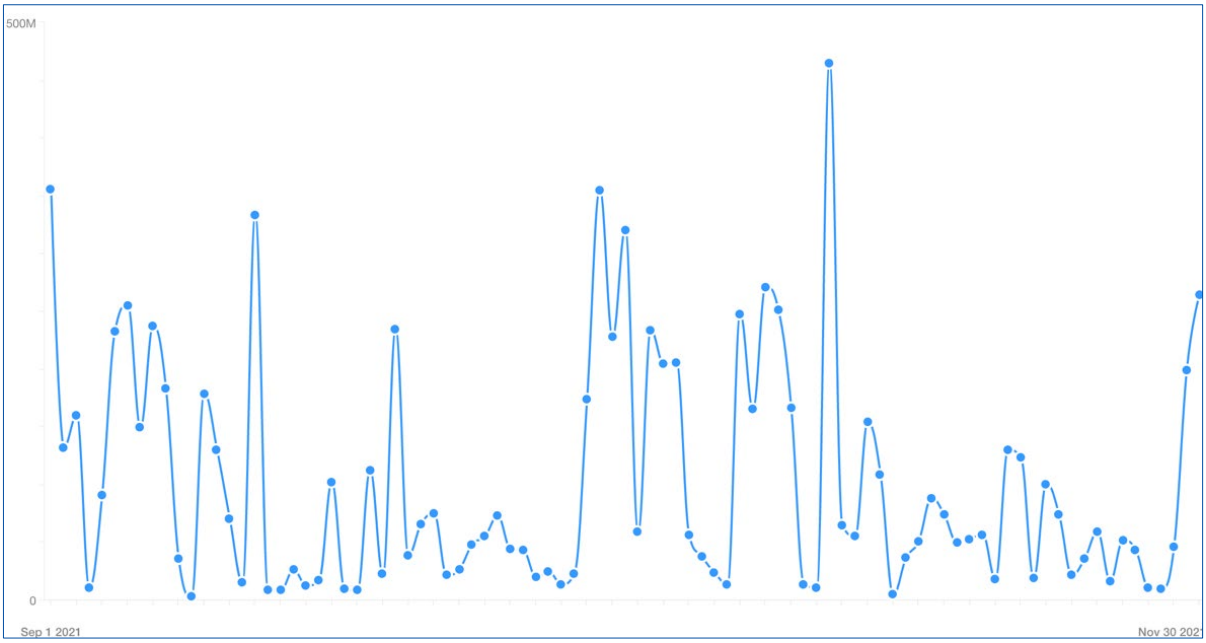
As well as reaching large social media audiences, ECSM also reached significant numbers of people through "traditional" publications such as newspapers. These results of media monitoring these mentions are shown in this section, as tracked by a media monitoring tool:

- The total number of mentions from 1 September to 30 November 2021 was **4,870 mentions**
- On average, **54 mentions occurred every day**



This mentions over time trend graph shows a big spike in mentions around the ECSM launch and press release distribution at the end of September. There were also regular spikes in mentions during ECSM itself in October.

The **potential reach was in the millions** due to the large audiences these publications have. It is difficult to discern a clear pattern as to when the peaks in reach were happening from the available data, but it is clear from this graph that the potential reach was very high on specific days before, during and after ECSM:



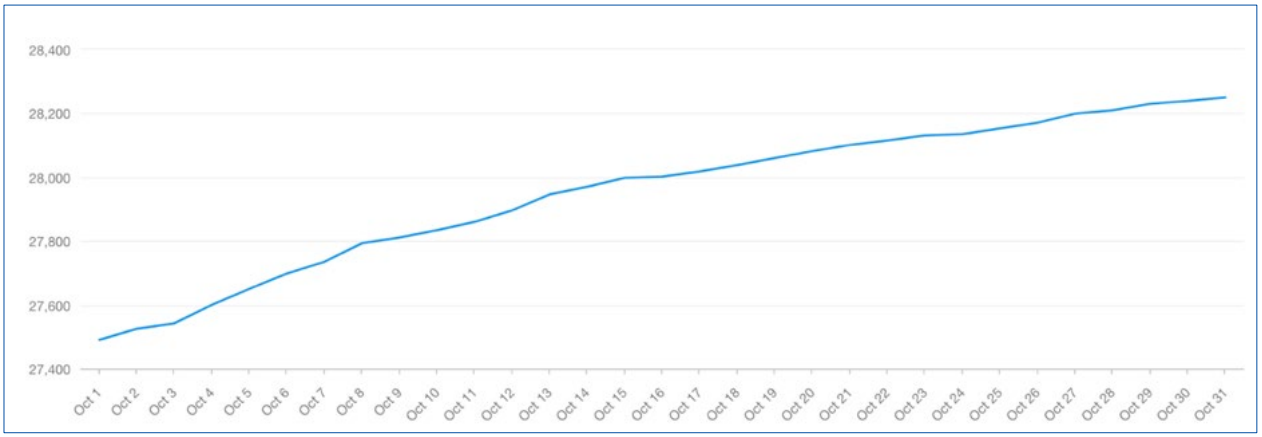
An analysis of the keywords that are used in these publications when they are writing about ECSM also gives valuable context. The word cloud below shows that "**security**" is the main word that comes up as would be expected, but that interesting sub-topics such as "**supply chain attacks**" and "**financial services**" also come up.

5.6 ASSESSMENT OF ENISA SOCIAL MEDIA RESULTS (ORGANIC AND PAID)

ECSM target audiences are very active on social media so this was a key way to reach them. This was achieved with both organic posts and paid posts, creating content centrally that was shared by ENISA as well as by the Member States in their own countries using translations that ENISA provided to them.

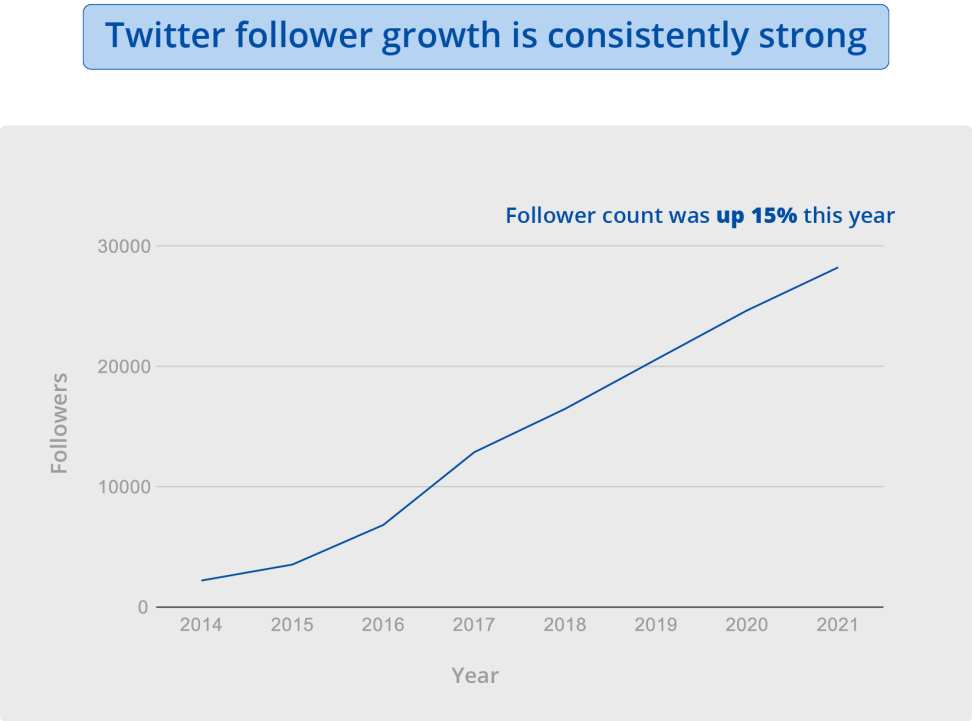
5.6.1 Daily growth of Twitter @CyberSecMonth followers

The official Twitter @CyberSecMonth account for the month was again a powerful tool for social media promotion. By looking at the increase in followers to the @CyberSecMonth Twitter account during ECSM 2021 shown in this graph, it can be seen that it increased steadily and consistently each day during the campaign. The biggest daily growth in followers was near the beginning of the campaign, with only a slight plateauing effect towards the end of the month showing that momentum was kept up throughout.



5.6.2 Annual number of Twitter followers of @CyberSecMonth

Strong growth in Twitter follower count was again a feature this year. It was up 15% on last year as can be seen in the chart here. The @CyberSecMonth account now has well over 28,000 followers.



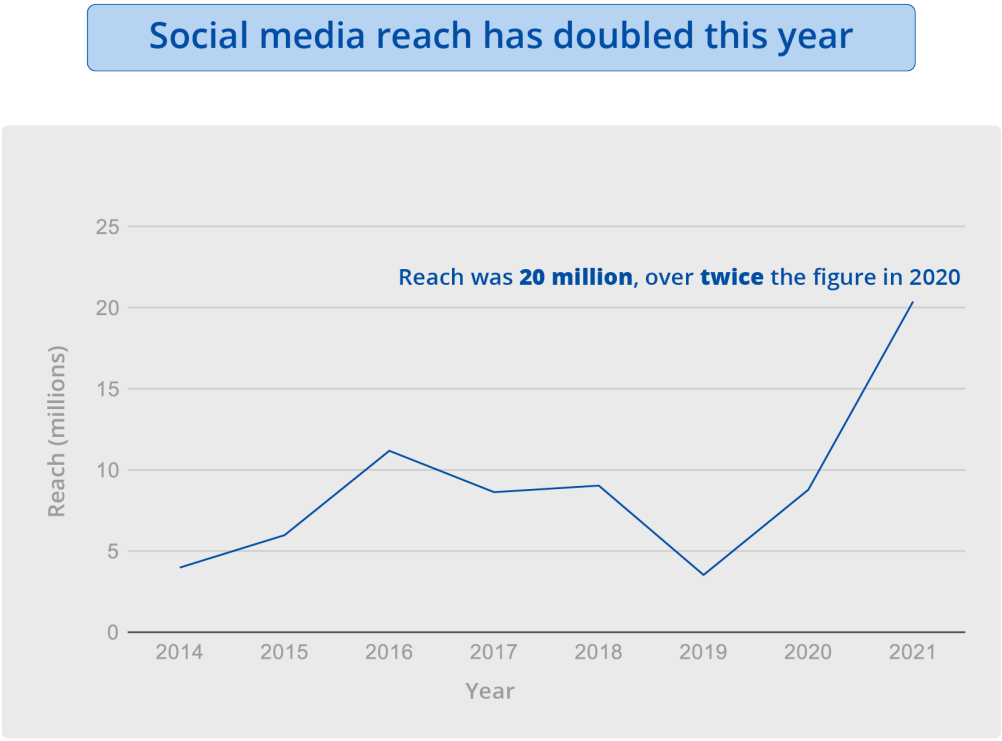
5.6.3 Social media reach

Social media was used as a listening tool to measure mentions of the #CyberSecMonth and #thinkb4uclick hashtags on social media and the wider web. This goes beyond measuring what was happening only on ENISA owned channels, and factors in how other people were using these hashtags and engaging with the campaign.

The headline figures are presented below. Notably they show **growth of over 3 times in mentions** overall, and **social media reach at over 20 million** (over twice the 8.8 million figure of last year):

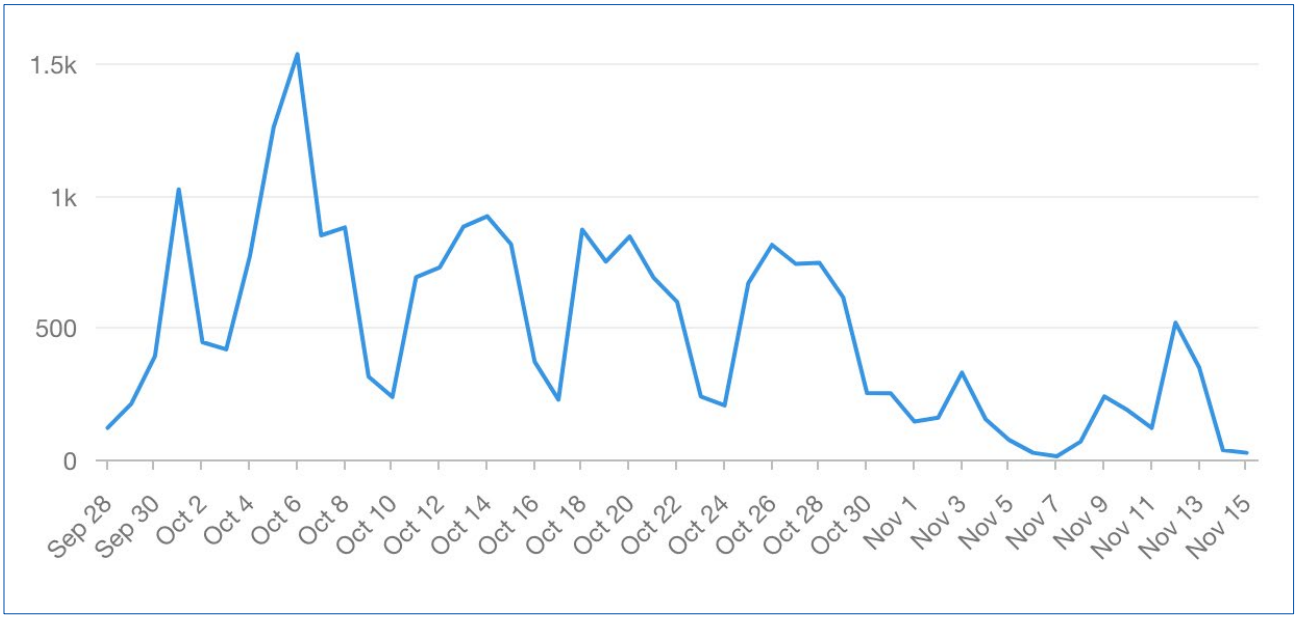
- Mentions 23,736
- Social Media Mentions 23,610
- Social Media Reach 20.4M
- Interactions 17,733
- Shares 17,290
- Mentions from Blogs 63
- Mentions from Twitter 22,700
- Mentions/Day Average 484
- Unique Twitter Authors 8.3k

This strong growth in reach is clearly shown in this chart giving an overview of the campaign's overall online reach from 2014 to 2021. These results are most likely due to the digital campaign strategy of combining enhanced content with increased paid social media spend that was optimised on an on-going basis.



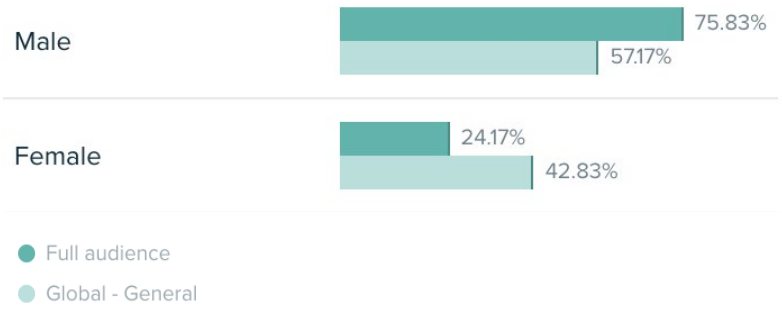
5.6.4 Daily Mentions

Looking at daily data, online mentions peaked at the beginning of ECSM 2021, and continued strongly throughout the month - and even beyond into November. Interestingly, most of the activity was happening on weekdays, with Saturdays and Sundays being noticeably quieter days:

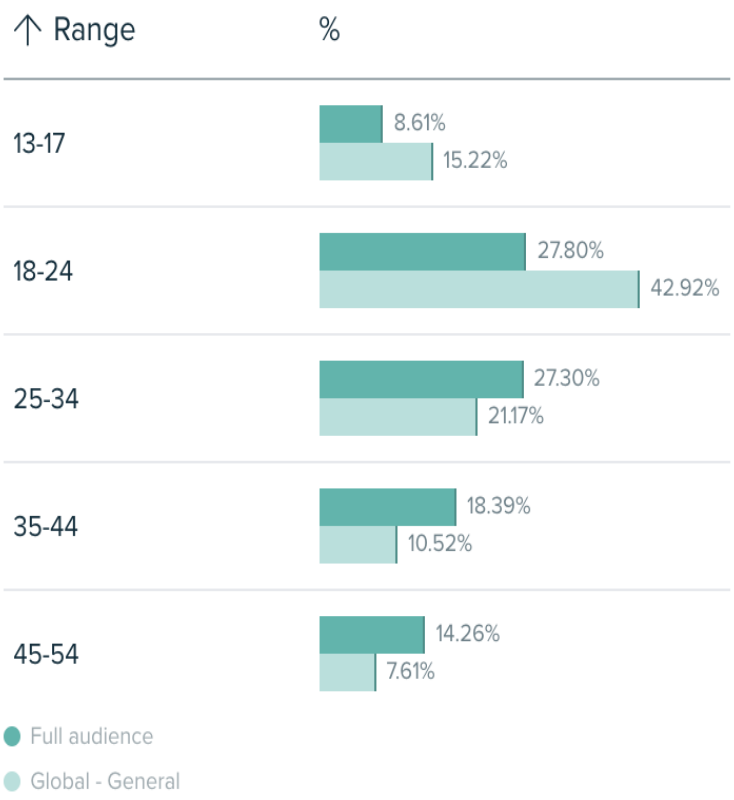


5.6.5 Twitter Follower Demographics

An online tool was used to infer the gender of ECSM Twitter followers. Interestingly, the ECSM campaign's "Full audience" skews more male (and less female) compared to the Twitter "Global – General" audience as shown in the screenshot below. This indicates that more males are following the ECSM Twitter account than would generally be the case for other accounts and can be used to inform the development of future campaign content.



The age distribution of ECSM followers is also interesting to note, with the largest cohort being aged between 18 and 34 years old and skewing slightly older compared to the general Twitter user profile. This shows that there is an opportunity for growth by creating content that appeals to younger people.



5.6.6 Top Keywords

Looking at the word cloud of the top keywords used alongside the campaign hashtags, we get clear picture of the top keywords used around the campaign topics. This gives us an insight into the types of content that is resonating with our audiences. For example, "**Tips**" is the keyword featuring most often indicating that people are engaging with useful guidance on best practice.

5.6.7 Top Entities

Interestingly, the EU was the "entity" most often mentioned on social media alongside the campaign hashtags, with ENISA itself also featuring prominently. This demonstrates the added value of a pan-European campaign in creating a shared sense of purpose in combatting cybercrime across Europe. It also shows how the ECSM campaign increases the awareness of ENISA's own work internationally.

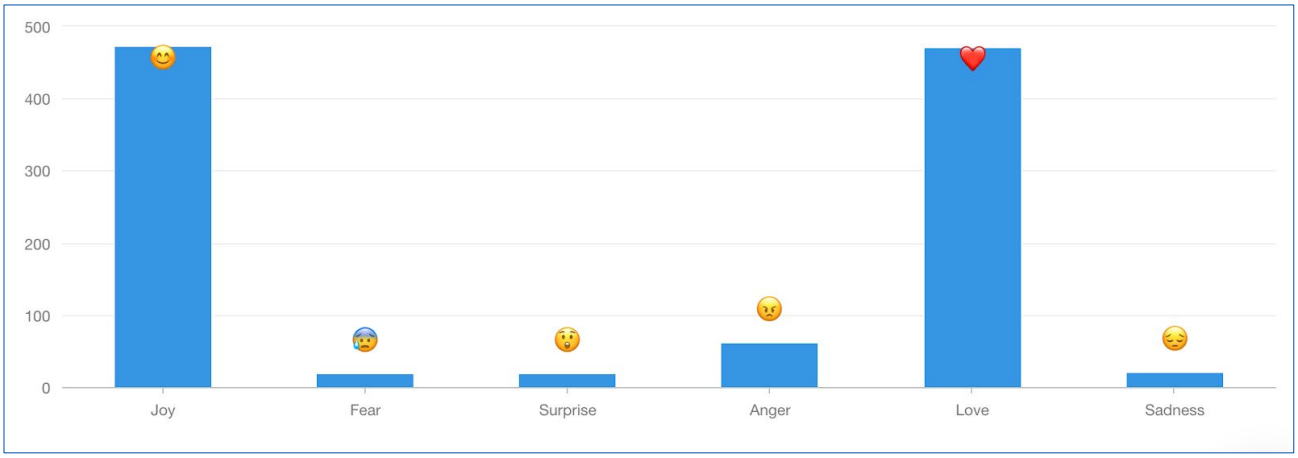
5.6.8 Sentiment

The sentiment of mentions is difficult to measure accurately because the automatic machine learning tools struggle to understand the context and nuances of human language.

However, we can see that many positive words are being used in the context of ECSM from the positive sentiment word cloud shown here.

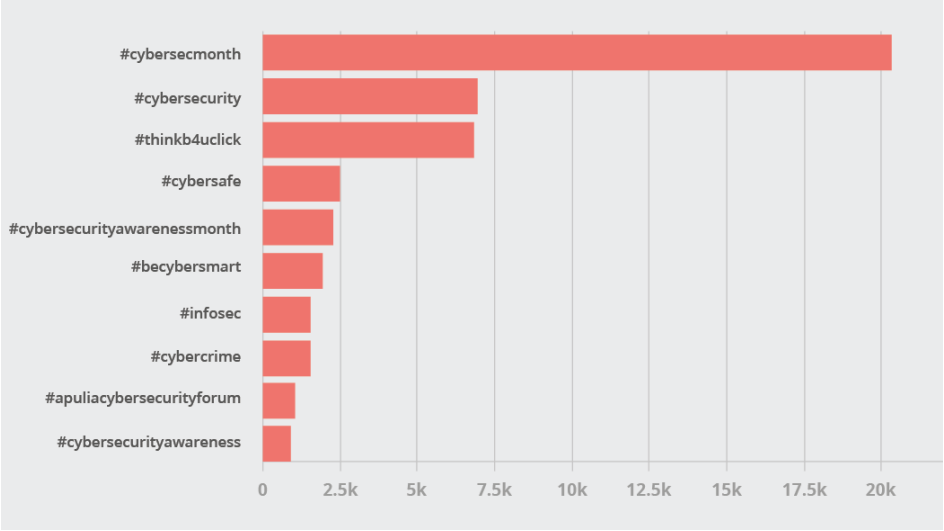
5.6.9 Emotional Comparison

Similarly, the emotions identified by the algorithm in mentions are also based on specific keywords, phrases and emojis and so should be interpreted with caution. Having said that, it is interesting to note that “joy” and “love” are the most prominent emotions suggesting that the campaign content was well received by the audience in general:



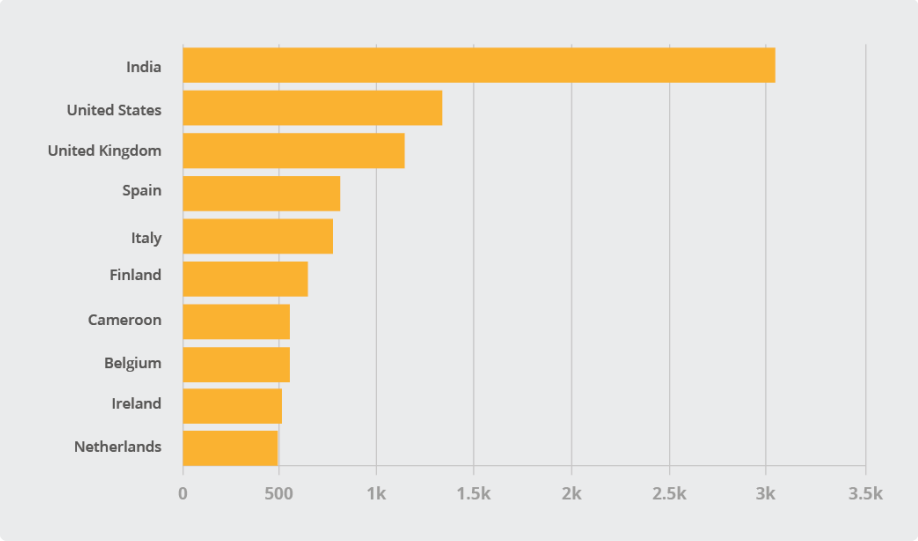
5.6.10 Top Hashtags

The main campaign hashtag of #cybersecmonth was by far the most popular campaign hashtag online. It is interesting to see that the #cybersecurity hashtag is effectively tied with #thinkb4uclick for second place. These top 3 hashtags are followed by other less frequently used hashtags such as #cybersafe and the much longer #cybersecurityawarenessmonth as shown in this chart:

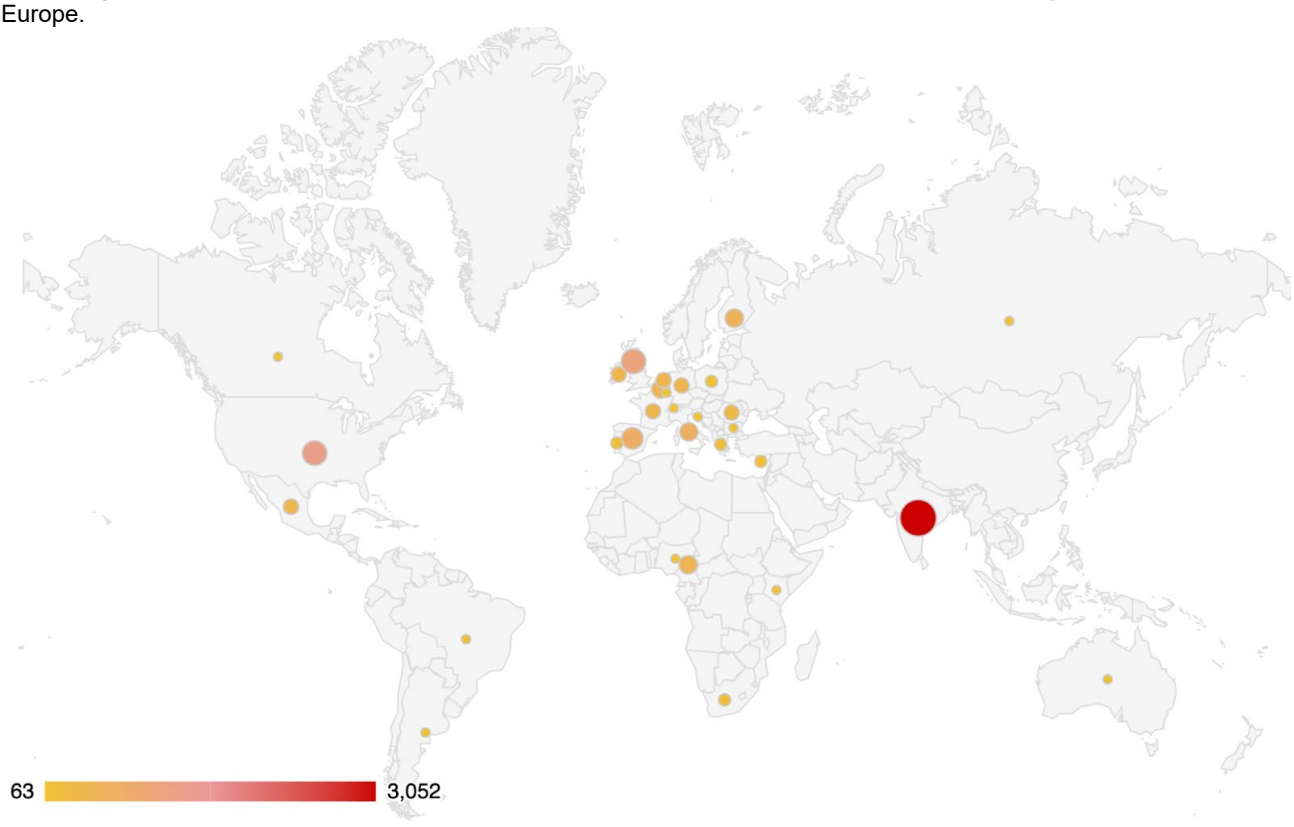


5.6.11 Number of campaign hashtag mentions per country on a worldwide scale

The global nature of cybersecurity can be seen most clearly in the list of top locations for mentions. India features very prominently - even more prominently than in previous years, with the United States and United Kingdom in second and third place. As is often the case, the figures for EU Member States and EFTA countries are measured on a country-by-country basis and not aggregated for the whole of the EU. This means that these individual countries follow larger population countries in the top locations table and the EU ranking is spread out. There is also a tendency for English language hashtags such as #CyberSecMonth and #thinkb4uclick to be used more in English speaking countries which would explain why English speaking countries are present in the top positions as shown below:



By looking at the distribution of mentions on a map as shown here, it is clear that most of the activity centres around Europe.

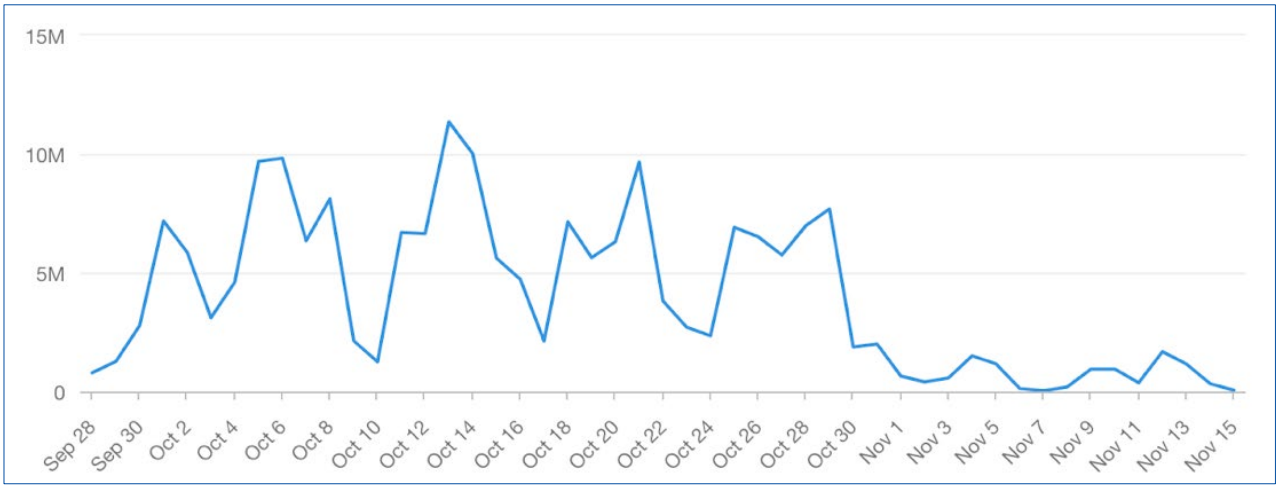


It would appear that India has the potential to distort our numbers because of its population size and close connections to the EU and UK computer industry, so it is useful to also report the metrics excluding India (and also excluding that popular “entry level interview” cartoon post mentioned earlier). But even with this constraint imposed, the social media reach figure in particular still shows a big increase - almost double what it was last year:

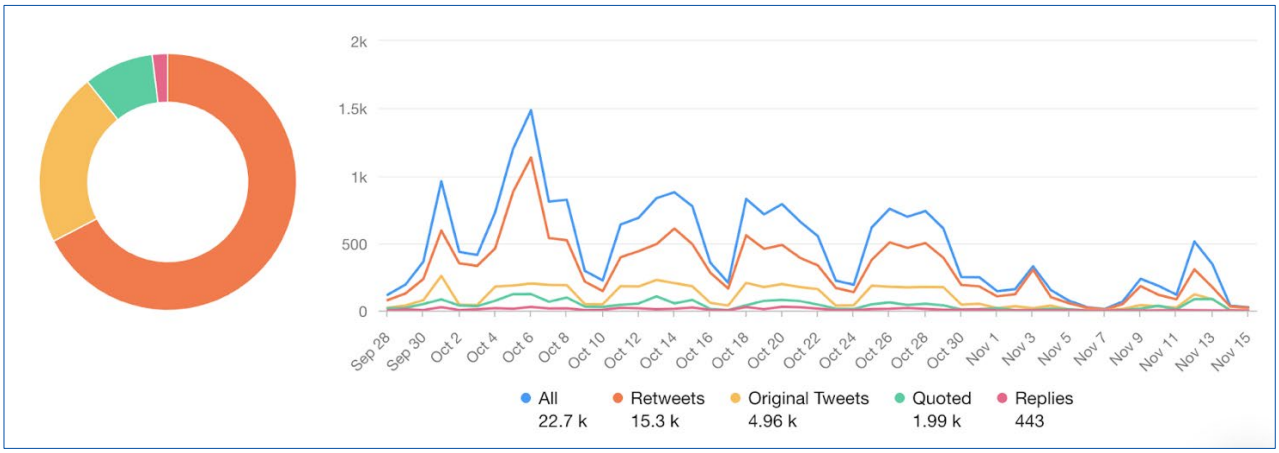
- Mentions 19,884
- Social Media Mentions 19,761
- Non-social mentions 123
- Social Media Reach 17.1M
- Interactions 14,100
- Shares 13,700
- Mentions from Blogs 62
- Mentions from Twitter 18,800
- Mentions/Day Average 406
- Unique Twitter Authors 6.77k

5.6.12 The Power of Twitter

Zoning in on Twitter specifically, we can see its power because it generated 196M impressions, with the same weekly periodicity mentioned earlier:



Comparing the types of tweets reveals the popularity of retweeting the content, with over 15,000 retweets and nearly 2,000 “quote” retweets.

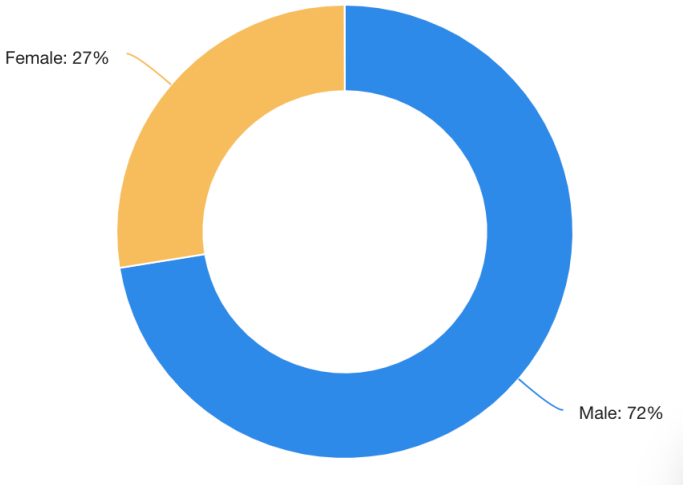


5.6.13 Emoji usage

Insights into the social media activity can also be gleaned by looking at the use of emoji around the campaign hashtags. The "**pointed finger**" and "**arrow**" emojis feature prominently, and these would often be associated with the sharing of tips or interesting information. Again, this shows how the audience was responding positively to the content being shared on social media:

5.6.14 Gender Breakdown

Although Twitter can deduce some information on gender from profiles, this should always be interpreted cautiously. Of those engaging with the campaign hashtags, there is a skew towards a more male audience, similar to that which could be seen with Twitter followers as shown in this screenshot from an online tool:



5.6.15 Paid post results

The campaign content was posted on social media both organically and supported by paid media spend. The top line results for the paid posts, measured from 30 September to 15 November 2021, as reported by the built-in measurement tools of the social media platforms themselves, are presented in the table below. These results show an **almost doubling in the important metrics of video views and engagement** compared to last year's figures. Website **clicks are also up significantly by nearly 5 times** year on year.

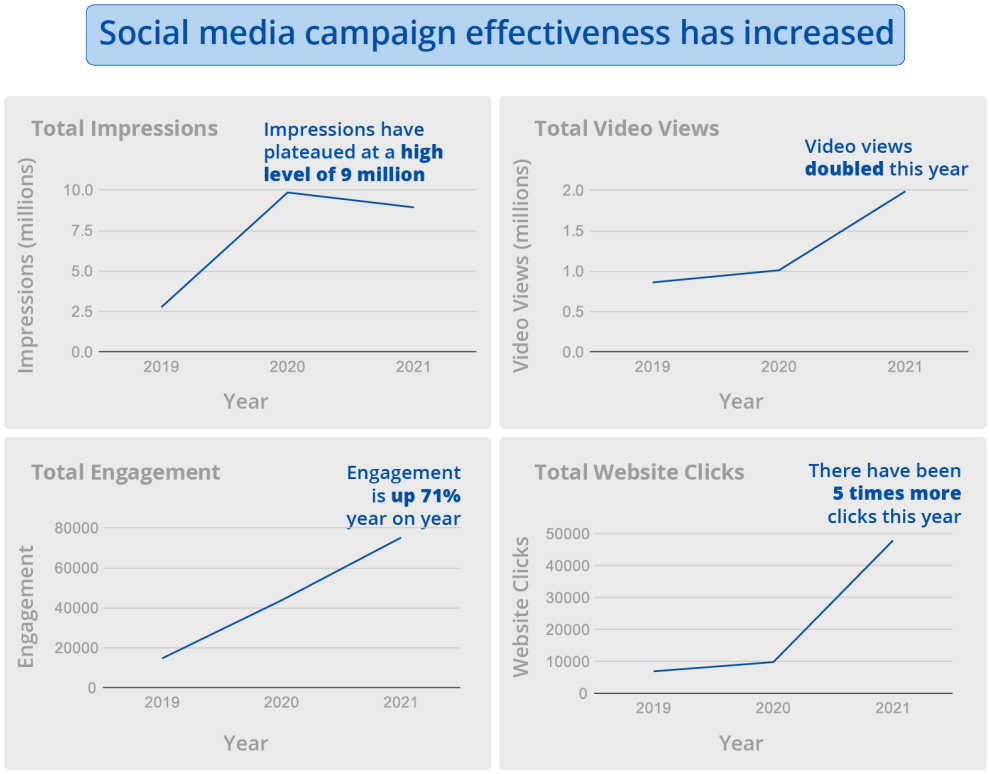
Effectiveness Metric	Communication Channel	Results
Impressions	**All**	**8,936,093**
	Facebook	3,792,522
	Twitter	3,637,525
	YouTube	1,506,046
Video Views	**All**	**1,988,673**
	Facebook	737,943
	Twitter	1,250,730
	YouTube	533,660
Engagement	**All**	**75,243**
	Facebook	36,545
	Twitter	32,599
	YouTube	6,099
Website Clicks	**All**	**47,939**
	Facebook	35,863
	Twitter	7,644
	YouTube	4,432

5.6.16 Comparison between previous years for the social media campaign effectiveness

This data shows that compared with previous years the paid advertising is becoming much more effective and driving significant increases in the metrics that matter.

These results include **video views up 97% year on year**, the figures for **engagement up 71% year on year** and **nearly 5 times as many website clicks** compared to last year's figures - all from a similar number of impressions.

The increase in video views can be attributed to the greater volume of video content and the increased paid budget used to promote them. The engagement metrics are being driven by this larger paid reach as well as the creative way in which the content is driving users to engage. Website clicks have gone up significantly with the greater focus on driving people to the website landing pages in order for them to access more content and resources.



6. CONCLUSIONS AND RECOMMENDATIONS

Year-on-year ECSM grows and develops. As the targets for ECSM are refined; as the methodology is improved and, as partnerships are extended, more people are reached more precisely in a way that makes a difference to them – and the results can be measured more effectively through the evaluation questionnaires and other metrics.

The goal of ECSM is to build a framework where cyber awareness in individuals and the “middleman” businesses and institutions that serve them leads everyone to behave in a cyber secure manner and to take cyber hygiene seriously.

In addition to the conclusions included in each of the earlier sections above, we can summarise the implications of the most important findings as follows:

- Member States highly value ECSM and see the potential impact of extend it beyond one month
- Digital channels are proving to be powerful ways of reaching audiences at scale
- Increased advertising budgets would mean that more people could be reached online
- More MS need to use knowledge assessment methods to measure the results of ECSM at national level

In terms of recommendations, some of the main ones emerging from the results are:

- The ‘Human Factor’ in cybersecurity awareness shall be further explored in order to provide more clarity on what drives behaviour change of users
- The evaluation framework shall provide the basis for comparabledata throughout the years both in terms of metrics and tools
- Physical in-person events are missed by many and their return to ECSM would be welcomed
- Young people and cybersecurity experts are two audience segments that could be targeted more
- NGOs could make valuable partners in the future - even more so than in 2021. These partnerships can provide the foundations, as well as the capability, for powerful interaction with users, the evolution of behaviour change and, ultimately, a more cyber secure world.

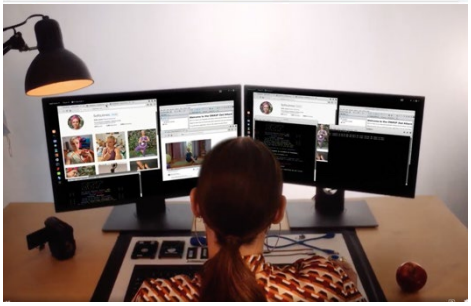
ECSM 2021 has shown the important opportunities opened up by deepening the understanding of the needs of the target audience and how best to engage with them in order to facilitate positive behaviour change. Ultimately, by taking the results and learnings from ECSM 2021 on board for future editions of ECSM, our shared cyberspace will become a safer place for us all to exist and thrive.

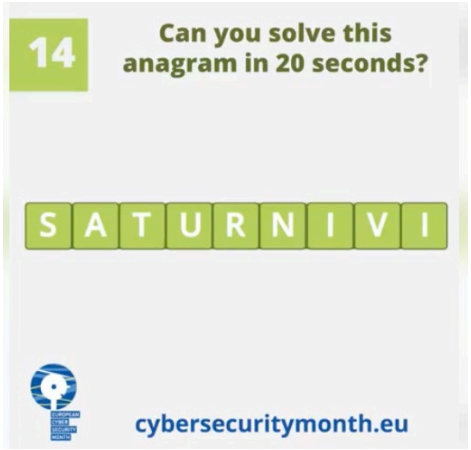
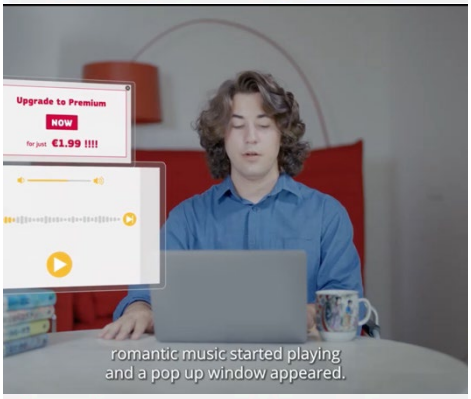
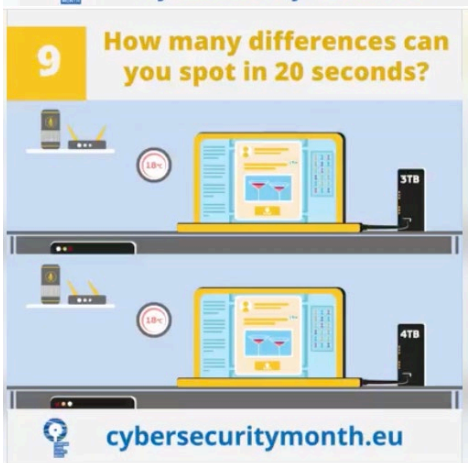
The on-going need for collaboration between Member States and organisations to create a wall of defence against increasing cybersecurity threats is clear. In that regard, European Cybersecurity Month 2021 can be considered a successful step on this ambitious journey.

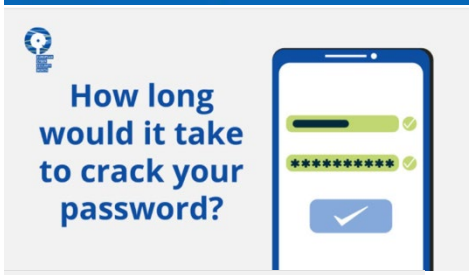
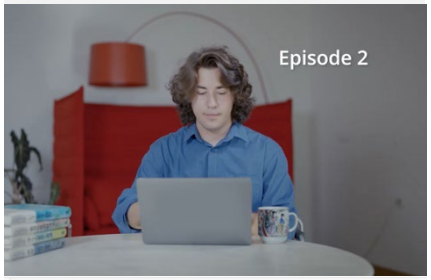
A ANNEX: MULTIMEDIA CONTENT SAMPLES

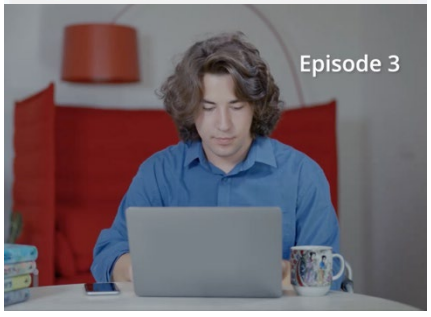
Here is a selection of the multimedia content produced along with clickable links to view them:

Date	Post Type	Creative	Post links (Facebook & Twitter)
28/09/21	"Coming soon" video		https://www.facebook.com/watch/?v=1233243770527369 https://twitter.com/CyberSecMonth/status/1442859452210679813
29/09/21	Text		https://www.facebook.com/CyberSecMonthEU/posts/578684873480722 https://twitter.com/CyberSecMonth/status/1443108279714992128
30/09/21	Video speech - Juhan Lepassaar		https://www.facebook.com/CyberSecMonthEU/videos/376274690804441/ https://twitter.com/CyberSecMonth/status/1443517820839632898
30/09/21	Video speech - Johannes Hahn		https://www.facebook.com/watch/?v=234852365351644 https://twitter.com/CyberSecMonth/status/1443627218639499266

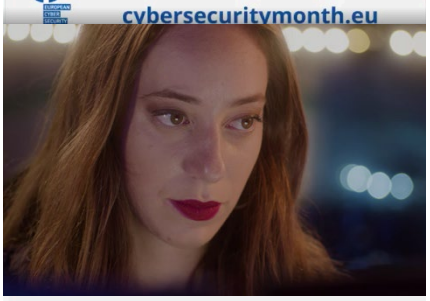
01/10/21	Video interview teaser		https://www.facebook.com/watch/?v=267744638547077 https://twitter.com/CyberSecMonth/status/1443973265056272384
04/10/21	Video teaser for infographic		https://www.facebook.com/CyberSecMonthEU/videos/602840910767871/ https://twitter.com/CyberSecMonth/status/1444983814581850125
04/10/21	Video Crossword		https://www.facebook.com/watch/?v=549484802819984 https://twitter.com/CyberSecMonth/status/1445048569816178688
05/10/21	Video cyber attack		https://www.facebook.com/CyberSecMonthEU/videos/270629074961619/ https://twitter.com/CyberSecMonth/status/1445337946866044935

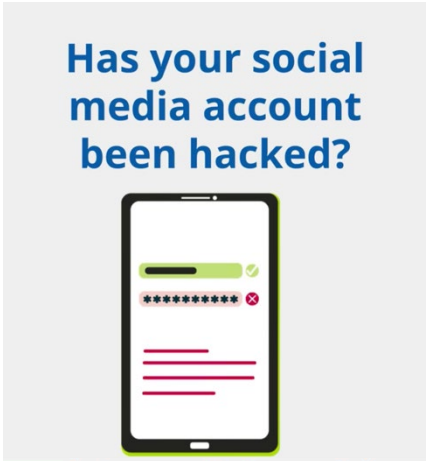
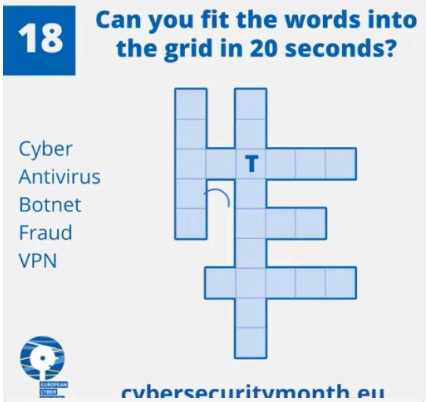
05/10/21	Video Anagram		https://www.facebook.com/watch/?v=393231409074822 https://twitter.com/CyberSecMonth/status/1445410956092362757
06/10/21	Video interview episode 1		https://www.facebook.com/CyberSecMonthEU/videos/2038553417165 72/ https://twitter.com/CyberSecMonth/status/1445665074236911622
06/10/21	Video criss-cross puzzle		https://www.facebook.com/watch/?v=1065300010967062 https://twitter.com/CyberSecMonth/status/1445771489081315333
07/10/21	Video spot the differences		https://www.facebook.com/watch/?v=600225770985217 https://twitter.com/CyberSecMonth/status/1446105804730478596

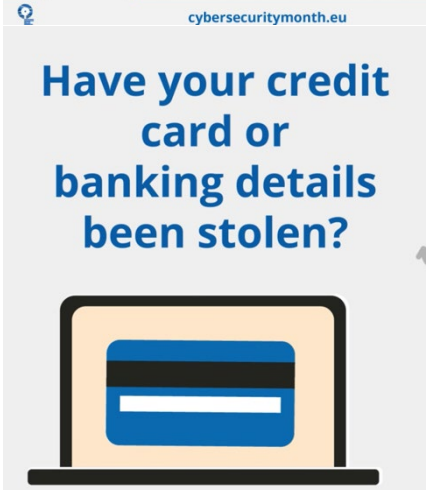
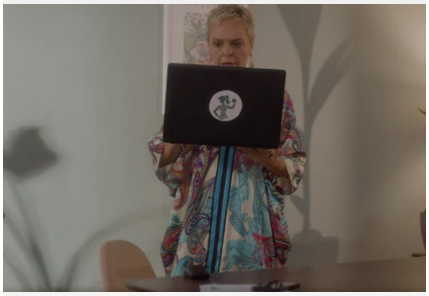
08/10/21	Video - teaser for infographic		https://www.facebook.com/CyberSecMonthEU/videos/953755868684063/ https://twitter.com/CyberSecMonth/status/1446405558559465492
08/10/21	Quiz - password		https://www.facebook.com/CyberSecMonthEU/posts/585350452814164 https://twitter.com/CyberSecMonth/status/1446499332962852864
09/10/21	Infographic 'Secure all your devices'		https://www.facebook.com/CyberSecMonthEU/posts/585361526146390 https://twitter.com/CyberSecMonth/status/1446777467188891652
11/10/21	Video interview episode 2		https://www.facebook.com/CyberSecMonthEU/videos/619248262419481/ https://twitter.com/CyberSecMonth/status/1447489721089904640
11/10/21	Video wordsearch		https://www.facebook.com/watch/?v=574694027184529 https://twitter.com/CyberSecMonth/status/1447585280370823168

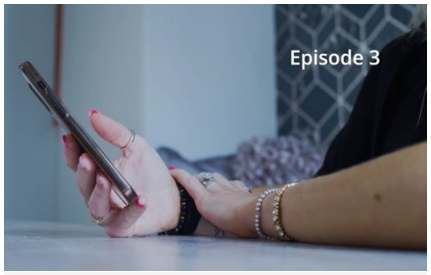
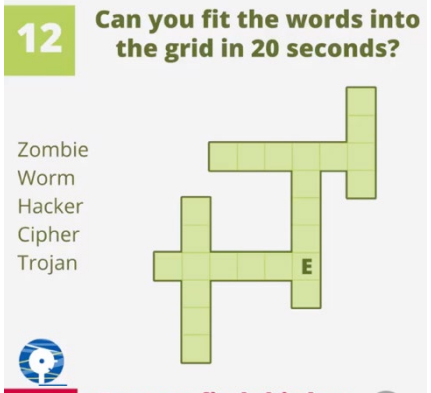
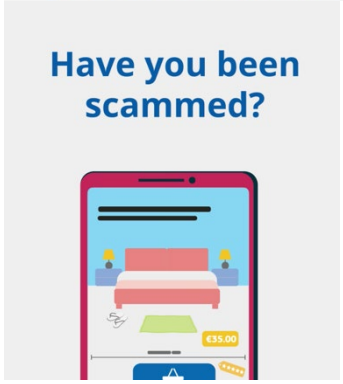
12/10/21	Video cyber attack		https://www.facebook.com/CyberSecMonthEU/videos/2954753641456859/ https://twitter.com/CyberSecMonth/status/1447839181670060035
12/10/21	Video puzzle		https://www.facebook.com/watch/?v=574306103872269 https://twitter.com/CyberSecMonth/status/1447947669150785538
13/10/21	Video teaser for infographic		https://www.facebook.com/CyberSecMonthEU/videos/579761246574233/ https://twitter.com/CyberSecMonth/status/1448195021635833859
13/10/21	Video criss-cross puzzle		https://www.facebook.com/watch/?v=177219774592935 https://twitter.com/CyberSecMonth/status/1448310059344093194
14/10/21	Video interview episode 3		https://www.facebook.com/CyberSecMonthEU/videos/247663433978238/ https://twitter.com/CyberSecMonth/status/1448546244746485765

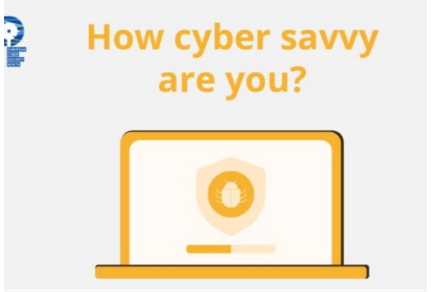
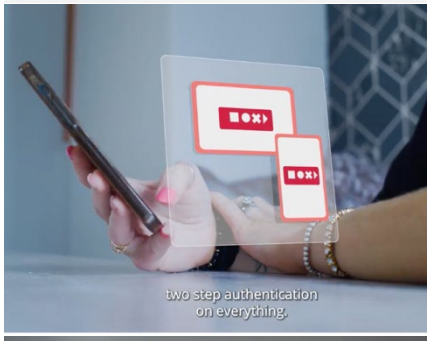
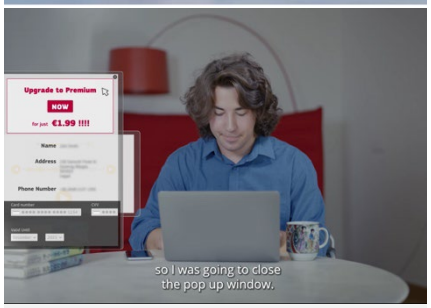
14/10/21	Picture - Ask the Expert coming up		https://www.facebook.com/CyberSecMonthEU/posts/589320875750455 https://twitter.com/CyberSecMonth/status/1448584506835968002
14/10/21	Video - Find the hidden key		https://www.facebook.com/watch/?v=1510199572686077 https://twitter.com/CyberSecMonth/status/1448672445443960835
15/10/21	Picture - Ask the Expert		https://www.facebook.com/CyberSecMonthEU/posts/589627229053153 https://twitter.com/CyberSecMonth/status/1448906489544908800
15/10/21	Picture - interactive map		https://www.facebook.com/CyberSecMonthEU/posts/589628065719736 https://twitter.com/CyberSecMonth/status/1448974433608028161
15/10/21	Quiz - cybersecurity skills		https://www.facebook.com/CyberSecMonthEU/posts/590117782337431 https://twitter.com/CyberSecMonth/status/1449008212695556104
15/10/21	Video teaser for interview 2		https://www.facebook.com/watch/?v=247002527456951 https://twitter.com/CyberSecMonth/status/1449034833011691521

18/10/21	Video interview episode 1		https://www.facebook.com/CyberSecMonthEU/videos/3011007932550510/ https://twitter.com/CyberSecMonth/status/1449993651468201984
18/10/21	Video puzzle		https://www.facebook.com/watch/?v=310378424318133 https://twitter.com/CyberSecMonth/status/1450121994922463233
19/10/21	Video cyber attack episode 3		https://www.facebook.com/CyberSecMonthEU/videos/906015430339969/ https://twitter.com/CyberSecMonth/status/1450356043289022464
19/10/21	Video puzzle		https://www.facebook.com/watch/?v=178832107761236 https://twitter.com/CyberSecMonth/status/1450484385568858114

20/10/21	Teaser for infographic		https://www.facebook.com/CyberSecMonthEU/videos/6199185766823410/ https://twitter.com/CyberSecMonth/status/1450743958829772808
20/10/21	Video word jigsaw		https://www.facebook.com/watch/?v=954066422127290 https://twitter.com/CyberSecMonth/status/1450846773635731458
21/10/21	Video - find the keys game		https://www.facebook.com/watch/?v=404929174464280 https://twitter.com/CyberSecMonth/status/1451205860001259523
22/10/21	Video interview episode 2		https://www.facebook.com/CyberSecMonthEU/videos/374255651095477/ https://twitter.com/CyberSecMonth/status/1451443209125703692
22/10/21	Quiz		https://www.facebook.com/CyberSecMonthEU/posts/594687965213746 https://twitter.com/CyberSecMonth/status/1451571410808225794

23/10/21	Image - Infographic		https://www.facebook.com/CyberSecMonthEU/posts/594705145212028 https://twitter.com/CyberSecMonth/status/1451820688369717248
25/10/21	Video teaser for infographic		https://www.facebook.com/CyberSecMonthEU/videos/2993407074257101/ https://twitter.com/CyberSecMonth/status/1452530367232036868
25/10/21	Video crossword		https://www.facebook.com/watch/?v=1492987561100763 https://twitter.com/CyberSecMonth/status/1452658712301092866
26/10/21	Video cyber attack episode 4		https://www.facebook.com/CyberSecMonthEU/videos/1038216597019749/ https://twitter.com/CyberSecMonth/status/1452892756066516994
26/10/21	Video puzzle		https://www.facebook.com/watch/?v=181687010713552 https://twitter.com/CyberSecMonth/status/1453021099285942272

27/10/21	Video interview episode 3		https://www.facebook.com/CyberSecMonthEU/videos/1008698923398891/ https://twitter.com/CyberSecMonth/status/1453255141021212672
27/10/21	Video - word puzzle		https://www.facebook.com/CyberSecMonthEU/videos/570401374019601 https://twitter.com/CyberSecMonth/status/1453383485779955714
28/10/21	Video - find the key game		https://www.facebook.com/watch/?v=958019441467933 https://twitter.com/CyberSecMonth/status/1453745877085036549
29/10/21	Video teaser for infographic		https://www.facebook.com/CyberSecMonthEU/videos/187820133494489/ https://twitter.com/CyberSecMonth/status/1453979917809553415
29/10/21	Image - podcast		https://www.facebook.com/CyberSecMonthEU/posts/598513504831192 https://twitter.com/CyberSecMonth/status/1453987466474520579

29/10/21	Image - UK reporter		https://www.facebook.com/CyberSecMonthEU/posts/598514574831085 https://twitter.com/CyberSecMonth/status/1454025221728612352
29/10/21	Image - Quiz		https://www.facebook.com/CyberSecMonthEU/posts/598468931502316 https://twitter.com/CyberSecMonth/status/1454108261670539273
30/10/21	Image - teaser fort infographic		https://www.facebook.com/CyberSecMonthEU/posts/598521494830393 https://twitter.com/CyberSecMonth/status/1454372508472430594
30/10/21	Video tip		https://www.facebook.com/watch/?v=616552109481467 https://twitter.com/CyberSecMonth/status/1454448001989046276
31/10/21	Highlights video		https://www.facebook.com/CyberSecMonthEU/videos/298818545194421/ https://twitter.com/CyberSecMonth/status/1454734896057004032
31/10/21	Image - final post		https://www.facebook.com/CyberSecMonthEU/posts/598482058167670 https://twitter.com/CyberSecMonth/status/1454825489026142211

B ANNEX: CONTENT CALENDAR EXAMPLE

This is a screenshot showing one of the content calendars that was used to coordinate online activities during the campaign:

ENISA EUROPEAN CYBERSECURITY MONTH 2021 CAMPAIGN
CONTENT CALENDAR FOR MEMBER STATES

UPDATED 11 OCTOBER 2021

	Date	Event	NOTES
CAMPAIGN LAUNCH	September 29	Inter-institutional kick-off event, Luxembourg, Co-organised by DG DIGIT and the European Court of Auditors https://www.eca.europa.eu/en/Pages/ECSM2021.aspx	
	September 30	Digital launch of the ECSM Commission interviews - Videos x 8	
	October 1	Award ceremony for the winners of the European Cybersecurity Challenge	
	October 1	Launch of EC animated video	

Theme	Date	NAME	Copy	NOTES
BE CYBER SECURE FROM HOME		Abbreviations used: BCSFH: Be Cyber Secure From Home CFA: Cyber First Aid		
	Monday October 4	1. Short teaser video for BCSFH Infographic 1 to send viewers to landing page with full infographic 'Top Tips to Make Your Home Cyber Safe' 2. Full BSCFH Infographic 1 published on landing page	From house alarms to fridges, all kinds of things can now be connected to the internet. Check out our infographic for tips on how to keep your home safe (url landing page) #CyberSecMonth #ThinkB4UClick	Infographic in 24 EU languages
	Tuesday October 5	Cinergies Video 1	Would you share private information online if you didn't know how it could be used? Watch our video to find out what could happen (url landing page) #CyberSecMonth #ThinkB4UClick	no dialogue - no subtitles
	Wednesday October 6	BCSFH Video - Episode 1	He never thought it would happen to him, but one day Patrik Pallagi discovered he'd been hacked! Find out what he did next (url landing page) #CyberSecMonth #ThinkB4UClick	subtitled in 24 EU languages
	Friday October 8	1. Short teaser video for BCSFH Infographic 2 to send viewers to landing page with full infographic 'Top Tips for Securing Your Accounts' 2. Full BSCFH infographic 2 published on landing page	How strong are your passwords? See our infographic for tips to help keep your accounts secure (url landing page) #CyberSecMonth #ThinkB4UClick	Infographic in 24 EU languages
	Monday October 11	BCSFH Video - Episode 2	What would you do if you'd been hacked? Watch Patrik Pallagi's full story here (url landing page) #CyberSecMonth #ThinkB4UClick	subtitled in 24 EU languages
	Tuesday October 12	Cinergies Video 2	Do you keep your digital devices updated? Watch our video to see the risks if you don't (url landing page) #CyberSecMonth #ThinkB4UClick	no dialogue - no subtitles
	Wednesday October 13	1. Short teaser video for BCSFH Infographic 3 to send viewers to landing page with full infographic 'Top Tips for Protecting Yourself Online' 2. Full BSCFH Infographic 3 published on landing page	More and more of us are connecting, sharing and communicating online. For advice on how to protect yourself online, check out our infographic (url landing page) #CyberSecMonth #ThinkB4UClick	Infographic in 24 EU languages
	Thursday October 14	BCSFH Video - Episode 3	After Patrik Pallagi was hacked, he took steps to ensure it wouldn't happen again. Find out what he learned from his experience (url landing page) #CyberSecMonth #ThinkB4UClick	subtitled in 24 EU languages

CYBER FIRST AID	Friday October 15	Cyber First Aid - New Interactive map	Check out our new interactive map to find local services you can contact if you are the target of online shopping fraud or social media account hack https://cybersecuritymonth.eu/cyber-first-aid #CyberSecMonth #ThinkB4UClick	
	Friday October 15	New ECSM Quiz	TBC - pending URL https://cybersecuritymonth.eu/quiz	
	Friday October 15	ENISA "Ask the Expert" session	TBC - pending further details	
	Monday October 18	CFA Video - Episode 1	Niamh Martin's social media account was hacked and held to ransom, here's what happened next (url landing page) #CyberSecMonth #ThinkB4UClick	subtitled in 24 EU languages
	Monday October 19	Cinergies Video 3	Did you know you can, and should, report cybersecurity attacks? Find out more by watching our video (url landing page) #CyberSecMonth #ThinkB4UClick	no dialogue - no subtitles
	Tuesday October 20	1. Short teaser video for CFA Infographic 1 to send viewers to landing page with full infographic 'Has Your Social Media Account Been Hacked?' 2. Full CFA Infographic 1 published on landing page	Would you know if your social media account had been hacked? And would you know what to do about it? See our infographic for tips and advice (url landing page) #CyberSecMonth #ThinkB4UClick	Infographic in 24 EU languages
	October 22	CFA Video - Episode 2	Niamh Martin's business was almost destroyed by hackers, watch her full story here (url landing page) #CyberSecMonth #ThinkB4UClick	subtitled in 24 EU languages
	October 25	1. Short teaser video for CFA Infographic 2 to send viewers to landing page with full infographic 'Have Your Credit Card or Banking Details Been Stolen?' 2. Full CFA Infographic 2 published on landing page	What would you do if you saw unusual activity on your credit card or bank account? Check out our infographic for advice (url landing page) #CyberSecMonth #ThinkB4UClick	Infographic in 24 EU languages
	October 26	Cinergies Video 4	Have you backed up your data? You will be very happy that you did if you are the target of a ransomware attack! (url landing page) #CyberSecMonth #ThinkB4UClick	no dialogue - no subtitles
	October 27	CFA Video - Episode 3	Niamh Martin shares what she learned after her business survived a ransomware attack. Watch her full story here (url landing page) #CyberSecMonth #ThinkB4UClick	subtitled in 24 EU languages
	October 28 TBC	CYBERSNACS Podcast - Interview with Demosthenes Ikonomou	TBC - pending further details	
	October 29	1. Short teaser video for CFA Infographic 3 to send viewers to landing page with full infographic 'Have You Been Scammed?' 2. Full CFA Infographic 3 published on landing page	Fake websites, fake ads, counterfeit goods... it can be easy to fall for a scam when shopping online. For advice on what to do, see our infographic (url landing page) #CyberSecMonth #ThinkB4UClick	Infographic in 24 EU languages

C ANNEX: CAMPAIGN STORIES

We present here the full individual Campaign Stories from around Europe.

European Commission

Cyber Aware Programme of the European Commission – EU Interinstitutional Cooperation

The European Commission (EC) is a high value target for cyber criminals and malicious actors interested in the information, financial and other assets it is managing. With the arrival of the COVID-19 pandemic, the number of attacks and cyber incidents reported increased by 50% in 2020 and the trend continues in 2021. With the newly adapted hybrid mode of working, from the office and from home, and the acceleration of the digital transformation, the digital surface to protect has significantly expanded.

In this challenging context, the corporate Cyber Aware programme organises activities and prepares and disseminates content to raise the awareness of the Commission staff on cybersecurity, all year round. In October, the European Cybersecurity Month (ECSM) is a crucial moment to promote the adoption of safe cyber practises.

Our target audience includes more than 35,000 colleagues. Most of them are based in Brussels or Luxembourg, some of them are working from other EU Member States. Many colleagues are not yet aware of their role as defenders of the Commission assets. Some of them do not know how to recognize and report a phishing email, create a strong password, which tools are available to transfer big files, etc. The ECSM offered the ideal opportunity to pass the message on ‘how to be cybersecure from home’, extremely topical for the people (tele)working for the European Commission. The ‘first aid’ topic offered the opportunity to inform staff on what to do and who to address when they fall victim to cyber scams in any of the EU Member States.

Building the 2021 messages

The Cyber Aware programme manager actively contributed to the work of ENISA with the Commission and the Member States in selecting the themes and building the messages for ECSM 2021 as well as preparing the material for use during the Month. The activities started already in March 2021 and involved regular online meetings to discuss and decide on the themes, messages and visual representation, as well as the timing and organisation of the campaign throughout the month.

Kick-off

Since 2018, the ECSM is kickstarted by the EU Institutions, Bodies and Agencies (EUIBAs) with an interinstitutional kick-off meeting. In 2021 the Commission teamed up with the European Court of Auditors (ECA) for the organisation of this event on 29 September. The objective is to raise awareness on cybersecurity and promote cybersecurity across all EUIBAs, and also to provide tips on how to stay safe online, protect data and on how to best act in case of a cyber incident. Speakers from different EU institutions and agencies shared their knowledge and experience. Of particular interest is the women only panel which put the spotlight on the role that women can play in meeting the skills gap in cybersecurity and raising the bar for upskilling in the field. The event took place in a hybrid format, online and in Luxembourg at the European Court of Auditors, open to the general public via web streaming. The session is still available on ECA’s website.

Activities

In the Commission, the Cyber Aware Programme geared up in delivering information sessions and management briefings to different Commission services, tailored to their specific needs. Live online training sessions were offered to all staff on the following topics: Are you Cyber Aware? Including a demo of a hack (in English and French), Mobile Cyber Hygiene and Audio and videoconferencing: your guide to safe and secure calls and meetings. As a special treat to celebrate the ECSM, each staff member received short, funny videos in their mailbox once a week. At the end of the month, a Cyber Aware Lunch Talk was organised with Stefania Chaplin, Solution Architect at Secure Code Warrior. The session was dedicated to Secure DevOps, the importance of change in the culture, and tips from the field on where to start.

Just before and at the end of the ECSM, we executed a phishing campaign targeting all Commission staff to raise their awareness on the dangers of phishing emails. The campaign included tips on how to spot the red flags in phishing emails and was followed by an invitation to complete a training module on videoconferencing scams.

Spreading the message

Several Commissioners and Commission VIPs produced short video messages offering advice on cybersecurity. These were shared on social media at the launch of the ECSM on social media.
Throughout the month and beyond, ENISA campaign's material was published on and distributed via the different Commission communication channels. Niamh Martin and Patrik Pallagi's stories and all other material was shared on the EC's intranet page, in articles and newsletters. The ECSM 2021 Quiz and the Cyber First Aid Map are still promoted, they are invaluable support also after October.

We engaged our "Cyber Ambassadors" to help spread cyber awareness across the Commission. The Cyber Ambassadors are participants of the Commission's inhouse Cybersecurity Training Programme, a learning path that helps staff to shift careers towards cybersecurity. They completed their cyber missions with enthusiasm and dedication, preparing awareness sessions, email campaigns, articles, quizzes, and offering tips on how to remain cyber secure to their colleagues. Many other motivated and inspired colleagues helped spread the word across the institution, including the Local Informatics Security Officer (LISO) in every Commission service. We all share the same mission to establish a cybersecurity culture across the board in the organisation.

Interinstitutional coordination and cooperation

Since 2020 European Institutions, Bodies and Agencies (EUIBAs) are seeking closer cooperation and exchange in the area of cybersecurity in the Cybersecurity Subgroup of the Interinstitutional Committee on Digital Transformation (ICDT). In this Subgroup, a Task Force (TF5) is dedicated to the area of cybersecurity awareness raising. The 11 EUIBAs collaborating in TF5 focus on sharing resources, information, knowledge, experience and best practises. This provided ENISA with an excellent platform to share with the community of EUIBAs the information about the preparatory activities for the ECSM and it gave the EUIBAs an early insight in and access to the promotional material and planning of activities during the ECSM.

The parties involved collaborated closely for the preparation, organisation and promotion of activities and events across EUIBAs for the ECSM, hence ensuring a spreading of messages across organisations and providing their staff the opportunity to access a wider array of information and events. As part of the TF5 work plan for 2022, increased coordination and preparation of joint activities for the ECSM is foreseen, including an interinstitutional kick-off event for the ECSM, a yearly tradition to continue.

Result

During the ECSM, we reached out to many colleagues in the European Commission, who are now more aware about safe practises and have received information to efficiently prevent and react to a cyber attack, particularly related to phishing emails. We observed a high number of participants in our live online sessions and events and a big increase in the number of visits to the Commission internal Cybersecurity Portal. The Cyber Aware Programme can count on a network of motivated advocates and Cyber ambassadors across the institution to help spread the messages.

The ECSM gave also a big boost to the interinstitutional cooperation in the area of cybersecurity awareness raising. For the first time so many different EUIBAs received early information and access to the ECSM resources and planning thanks to the platform for exchange and cooperation provided by the Task Force dedicated to awareness raising across EUIBAs.

Conclusion

Neither citizens nor staff members of organisations and companies should be left alone when dealing with cybersecurity. Staff should have regular access to training sessions and awareness raising materials to confront the increasing number of cyber attacks, which become more and more sophisticated and oftentimes use social engineering techniques.

The activities and networks deployed by the European Commission Cyber Aware Programme are maintained throughout the year and are an excellent base from which to launch a more intense campaign of activities, events and messages which we look forward to start preparing early 2022, to be launched during ECSM 2022.

Campaign Visuals
Throughout the Month, the visual materials provided by ENISA were used.

Promotion for the short funny training videos, “The Cyber Guys”:

Capture of video messages from Commissioner Hahn and the Director-General of DIGIT Mario Campolargo:

Cyber Aware Lunch Talk promotion:

Visual of a cyber mission by the Cyber Ambassadors:

Interinstitutional kick-off event for the ECSM one page agenda

Interinstitutional kick-off event for the European Cybersecurity Month (ECSM)

On the road to cyber mature organisations with cyber aware staff

29 September 2021 – 10.00-16.00
@European Court of Auditors (ECA) – Hybrid event

Register in EU Learn here

EUROPEAN CYBER SECURITY MONTH

CYBERAWARE

Agenda

Morning session

Warming up with video presenting the ECSM

10.00 – 10.15 **Opening of the session**
Iliana Ivanova, Member of the European Court of Auditors, Dean of Chamber II, Investment for Cohesion, Growth and Inclusion

10.15 – 10.30 **The European Court of Auditors and cybersecurity-related audits**
Zacharias Kolias, European Court of Auditors Secretary-General

10.30 – 10.35 **Video Message by Commissioner Johannes Hahn**

Moderator: Magdalena Cordero, Director of the Directorate for Information, Workplace and Innovation, European Court of Auditors

10.35 – 11.55 **Spotlight on Women in Cyber**
- Christiane Kirketerp de Viron, Member of the Cabinet of Commissioner Johannes Hahn
- Ann Mennens, Manager Corporate Cyber Aware Programme, European Commission
- Maria Bouligaraki, Head of Planning and Standards Unit, EU-LISA
- Rosanna Kurrer, Cofounder and Managing Director of CyberWayFinder
- Krystina Gray, Vice-President of Women4Cyber Luxembourg Chapter and Women Cyber Force

11.55 – 12.00 **ECSM video**

Afternoon session

14.00 – 14.35 **Introduction to the ECSM, its role and activities**
- Juhan Lepassaar, Executive Director of the EU Agency for Cybersecurity (ENISA)
- Lorena Boix Alonso, Director Digital Society, Trust & Cybersecurity, DG CONNECT, European Commission
- Pascal Steichen, CEO of SECURITYMADEIN.LU

14.35 – 15.05 **Common cybersecurity rules for EUIBAs**
- Dr Ken Ducatel, Director DIGIT.S "IT Security", European Commission
- Saâd Kadhi, Head of CERT-EU
- Walter Petrucci, Director-General DG ITEC, European Parliament, and Chair of CERT-EU Steering Board

15.05 – 15.10 **ECSM video**

15.10 – 15.50 **Secure@home**
- Raluca Peica, Director Information Technology, Court of Justice of the European Union
- David Galloway, Deputy Director-General, Digital Services, General Secretariat of the Council
- Edvardas Šileris, Head of European Cybercrime Centre, Europol
- Mário Campolargo, Director-General, DG DIGIT, European Commission

15.50 – 16.00 **Outcome of surveys - Closing remarks**

#CyberSecMonth
#ThinkB4UClick

Our logo and visual identity:

Bulgaria

Exposition

It is the 4th year in a row in which the State e-Government Agency of Republic of Bulgaria (SEGA) coordinates and organises a specific campaign for ECSM at national level. Through the years, in sync with ESCM, we focused on different topics but also had a national focus on different cybersecurity themes. We've managed to build some long term partnerships for this campaign – GDBOP (Chief Directorate for Fight against Organised Crime) and Sofia Municipality (Metropoliten) are both our long term partners in raising awareness and campaign messages. Each year we aim to upgrade the campaign with new partnerships by reaching out to different organisations in the NGO sector, academia, business and other institutions. Following the guidelines for this year's campaign, SEGA has, for the first time, invited popular Bulgarian actors to become ambassadors of the campaign. Alexandra Sarchadzhieva and Kitodar Todorov, are Bulgarian actors, who are very recognizable from the stage and screen but also have a lot of followers online. Throughout the month they both shared various messages, infographics and advice from the campaign on their social media accounts; they were moderators in discussions on the topic of cybersecurity; they made video messages for their audience; and invited interesting guest experts to discuss cybersecurity issues.

The partnership with our ambassadors was very successful. With the help of their social media presence we managed to reach a large and extremely diverse audience and because they themselves were not experts in the field of cybersecurity, they managed to "take a journey" through the topic and the advice they shared made these topics more understandable for people.

Due to the pandemic, SEGA-organised events took place mainly online as webinars where different aspects of cybersecurity and different points of view were presented and considered. In the end the average consumer and citizen received useful advice for their safe online presence.

As ECSM campaign coordinator for Bulgaria, I believe our efforts to improve information on cybersecurity practises have had the desired impact. Information and awareness is definitely a prerequisite to changing behaviour but more is needed to build up good online habits and cyber culture. This is why such campaigns have to be implemented in conjunction with other strategies throughout the year, something we are considering. We believe that a winning strategy going forward would include the concept of learning by doing; show cases from real life situations; continually supplying people with real information on trends; and teaching them basic terminology and practises.

Problem

Bulgarian cyberspace does not differ greatly from its European counterparts and as such it has similar problems. Of course, it has its idiosyncrasies, which alongside the main trends, we have tried to reflect on this year.
In the last 5 years internet usage in Bulgaria has increased, and during this period the number of mobile broadband users has quadrupled. The positive trend of penetration and development of Internet access and related technologies creates a number of challenges around the lack of skills for using digital technologies and exposes Bulgarian citizens to unknown risks and threats. The latter includes: threats to physical safety, especially for children and seniors, threats to privacy and personal information, card theft and payment fraud, etc.
Through the experience SEGA gained from its core mission and main duties, and having analysed all the various data available we concluded that this year the campaign should focus on a few specific issues:

- Basic steps in cybersecurity for small and medium enterprises (SME), which are essentially the backbone of Bulgarian (and European) economy. SMEs are subjected to the same cyber risks as bigger companies but often do not have the human and financial resources to counter the cyberattacks. At the same time, they often lack information on this topic.
- Cybersecurity in municipalities. The difficulty and lack of (human) capacity to cover and execute the minimum requirements for network and information security.
- Addressing the lack of experts in cybersecurity and IT.
- The necessity to encourage the efforts in our country to join international initiatives and projects, as well as to upgrade the interinstitutional interaction.
- The need for general information and awareness.

Resolution

Cybersecurity in SMEs
A joint online poll was created among SMEs together with the Bulgarian Small and Medium Enterprises Promotion Agency. Its main goal was to establish the general level of awareness and preparedness in the field of cybersecurity. After that, we organised an online meeting in which the poll results were presented, experts commented on the data and gave advice. At the end of the campaign, all companies that participated in the poll were given the opportunity to receive a personal consultation via telephone or in an online meeting with cybersecurity experts.

Cybersecurity in Municipalities
This topic was presented in an online meeting with SEGA experts, as well as with guests from the two biggest municipalities in the country - Sofia Municipality and Plovdiv Municipality. The discussion focused on difficulties, challenges, possible solutions and good practises, as well as on the capabilities for technical and expert help, which the municipalities can receive from SEGA and the central government; contact points, training opportunities and usage of joint resources were also presented.

The Lack of Experts in Cybersecurity and IT
We organised a series of online meetings which dealt with different aspects of the problem. Opportunities for education and career advancement were discussed with representatives of universities, offering master courses and educational programs. An NGO, representing a large portion of the IT community in the country presented an initiative of its own, in which independent IT experts, engaged in all sectors of the state. We also organised a special event, dedicated to women in cybersecurity and IT. The event was moderated by one of our ambassadors, a popular Bulgarian actress. We wanted to address the necessity of having more women pursue a career in the digital world and to smash the stereotype that this is “a man’s world”. We began with the inspiring story of Ada Lovelace, considered by many to be the first programmer in the world and we presented the personal stories of three successful women from the SEGA team, who chose a career in technology and we hope that we have inspired other women to pursue a career in this field. This topic got really positive feedback. Bulgaria leads in a very positive statistic in Europe - the ratio of men and women working in tech. This trend needs to be encouraged and supported.

International Initiatives and Projects
SEGA took part in the realisation of “InfoSec SEE 2021 Cybersecurity Resilience and Adaptation”. This is the largest conference dedicated to cybersecurity in the Balkans. There, we presented the updated National Cybersecurity Strategy, the updated Road Map, which accompanies it, as well as guidelines for developing an Integrated National System for cybersecurity. We organised an online conversation with experts, where we presented four EU projects ECHO, CS4E, CONCORDIA, and SPARTA. A meeting between the people occupying the position of the National Coordinator for cybersecurity occurred for the first time. The current one being the chairman of SEGA. He and his three predecessors exchanged ideas and experience and agreed on the message that cybersecurity requires continuity, group decisions, cooperation and information sharing. World, European and national cybersecurity issues were discussed and a clear message was sent to society that good cyberculture must be a part of our everyday habits and we must keep up a certain cyber “hygiene”.

General Information and Awareness
An online meeting was conducted in which experts commented on the most common cyberattacks during the Pandemic.
We organised a meeting with ethical hackers, who told us more about that profession. What their role is, what techniques they use and when we can seek help from them. They also demonstrated hacker techniques live on-air and gave advice to citizens.
Many short videos were made with the ambassadors, who also hosted events with experts on their social media channels.
We created extra infographics and quizzes in addition to those supplied by ENISA, and we developed daily online content for the social media accounts of SEGA.
We hosted a meeting with the topic “Cybersecurity for children and parents”. Bulgarian children spent a lot more time online compared to their peers in the EU. Bulgarian parents allow their children to go online as early as the age of three. The event addressed: the need for every child to be protected in the digital world, that digital and cyberculture must be nourished and encouraged throughout our whole lives and that this is a process in which school and institutions are not the only ones responsible; parents also have an important place in this process.

Result

For the ECSM 2021 campaign, the State e-Government Agency (SEGA):

- Organised 13 online events, aimed at specific target audiences.
- We achieved an average viewership of 600 people per video meeting, with views ranging from 200 to 1,700 viewers.
- We introduced people to some essential terms, some basic and some advanced advice and tips on how to be secure online.
- In cooperation with Sofia Metropoliten, the campaign videos were shown during the entire month of October, in all metro stations, 30 times a day, thus reaching a wide range of the public.
- We managed to get a lot of interest and positive feedback from a large portion of our audience.
- We created a special section on SEGA’s website, dedicated to the campaign, as well as an interactive calendar which included all the events and all the presentations of guests and organisations. We also managed to create a special section from where anyone can download and use any of the campaign materials - videos, infographics, etc.
- We produced a special practical brochure, dedicated to one of the most common cyberattacks - ransomware.

- The campaign attracted significant interest and a large new audience for our Facebook page - every week we registered a rise of approx. 100 new followers.

Conclusion

Generally, citizens and businesses demonstrated interest towards the topics and discussions that SEGA had presented throughout the ECSM campaign. We believe that the interesting experts, ambassadors and guests, as well as the talk-show format chosen for our meetings and conversations became very appealing and watchable for our audience. This shows that as long as there is an on-going discussion of cybersecurity risks and awareness, the target audience will eventually adopt cybersecurity advice as an essential part of their online presence and behaviour.

Campaign Visuals

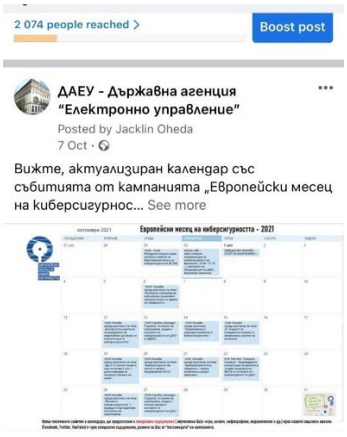
FACEBOOK POSTS:

Post about the kick-off event for the ESCM-2021

30.10.2021 – COUNTDOWN – 1 day left

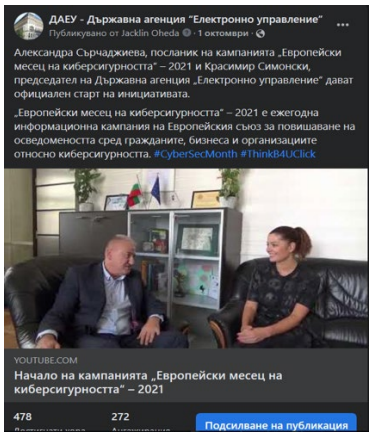
"Be cyber smart, create strong passwords for each of your accounts."
ONE DAY
till the start of the
"European Cybersecurity Month 2021"

Post with interactive calendar – it was updated several times afterwards with more events added to it.

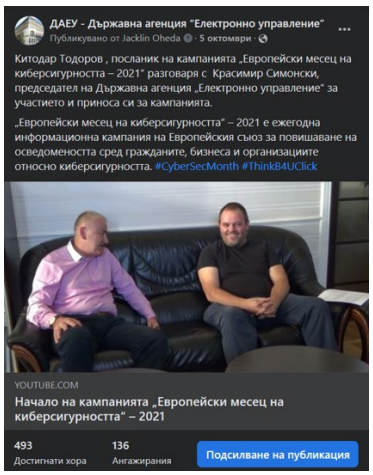


Uniting to raise awareness on cyber threats, the European Union Agency for Cybersecurity (ENISA) is launching the "European Cybersecurity Month 2021" campaign #CyberSecMonth #ThinkB4UClick https://www.enisa.europa.eu/…/cnect-2021-00359-02-00-bg-tra…

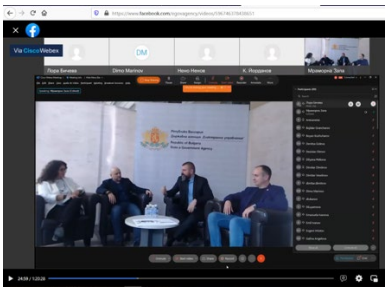
VIDEO - Alexandra Sarchadzhieva, ambassador of the campaign and Krasimir Simonski, Chairman of State e-Government Agency (SEGA), gave an official start to the campaign. #CyberSecMonth #ThinkB4UClick



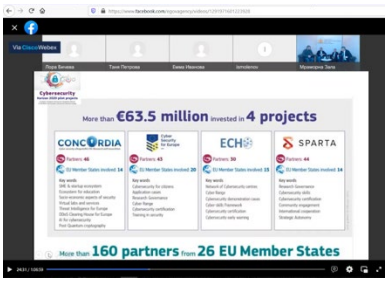
VIDEO - Kitodar Todorov, ambassador of the campaign and Krasimir Simonski, Chairman of State e-Government Agency (SEGA) - addressing the issue with the cybersecurity and the key message of the campaign. #CyberSecMonth #ThinkB4UClick



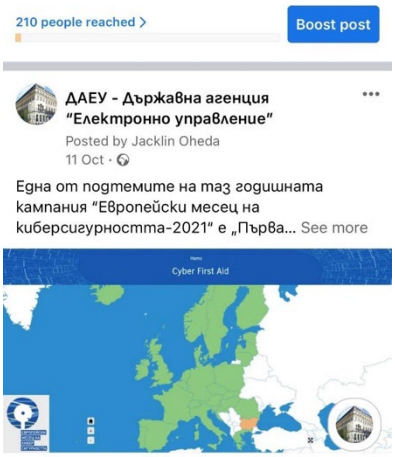
Online meeting on the topic of different trends in cyberattacks and how they changed during the pandemic. Experts : Peter Kirkov, Director Network and Information Security, SEGA; Miroslav Stefanov, Expert in Network and Information Security, SEGA; and Chief Inspector Svetlin Lazarov,Head of Digital Analyzes and Open Sources Sector at the Cyber Crime Department of the General Directorate for Fighting Organised Crime at the Ministry of Interior.



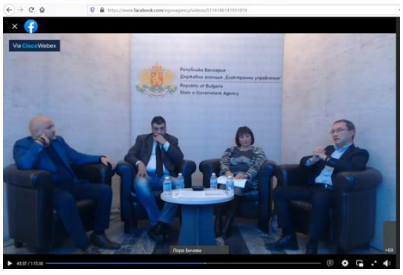
Online meeting where we presented four EU projects ECHO, CS4E, CONCORDIA, SPARTA. Experts : Col. Assoc. Prof. Dr. Nikolay Stoyanov, Deputy Director of the Institute of Defence "Professor Tsvetan Lazarov"; Borislav Sestrimski, over 20 years of experience in system integration, development, implementation and maintenance of processes, project management in IT; Assoc. Prof. Dr. Eng. Boyan Zhekov, official representative of Bulgaria in the program committees of Horizon Europe: 1. Civil security for the society (including Cybersecurity); 2. Digitalization, industry, space; Peter Kirkov, Director Network and Information Security, SEGA



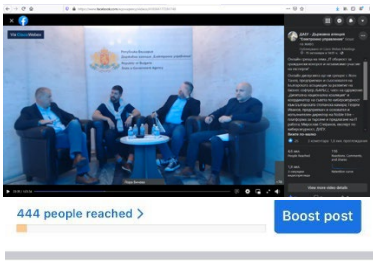
Post presenting the interactive map Cyber First Aid

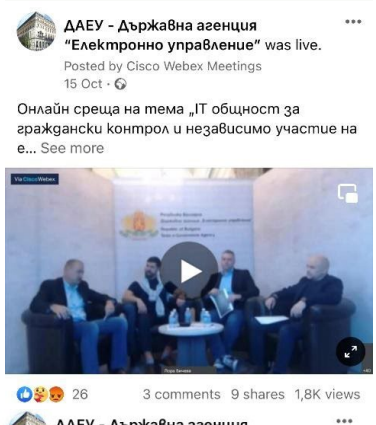


Online meeting on the topic of Cybersecurity education – master programs, discussed with representatives of universities, offering master courses and educational programs. Experts: Assoc. Prof. Dr. Eng. Boyan Zhekov, Deputy Dean of the Faculty of Information Sciences (FIN) at the University of Library Science and Information Technology (UniBIT) and Head of the Master's Program "Cybersecurity and Digital Forensics"; Assoc. Dr. Pavlinka Radoyska, Higher School of Telecommunications and Post; Nedko Tagarev, Chief Assistant at the Department of National and Regional Security at the University of National and World Economy.

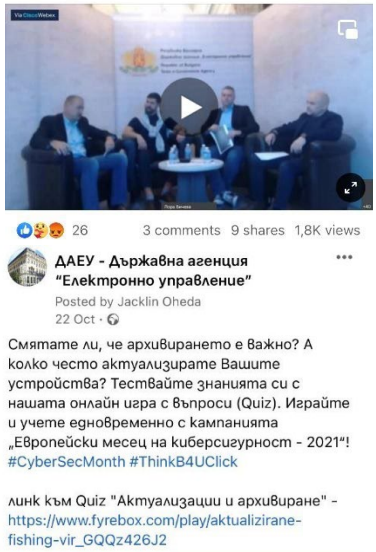


Online meeting on the topic of "IT community for civilian control and independent participation of experts". Experts: Jasen Tanev, entrepreneur and co-founder of the Bulgarian Association of Software Developers (BASD), member of the association "Digital National Alliance" and coordinator of the Cyber Security Council at the Bulgarian Chamber of Commerce; Georgi Ivanov, Founder and CEO at Noble Hire - a referral-based job marketplace; Krasimir Simonski, Chairman of State e-Government Agency (SEGA), Miroslav Stefanov, Expert in Network and Information Security, SEGA .

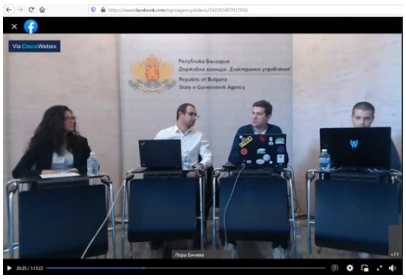




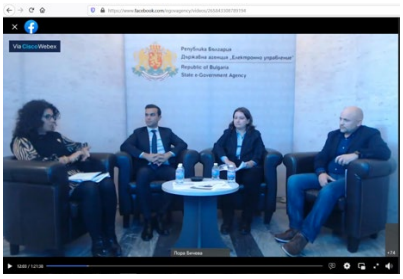
How to protect your digital privacy? Test your knowledge with our online Quizzes.
https://www.fyrebox.com/…/pravilno-li-sa-zashiteni…/



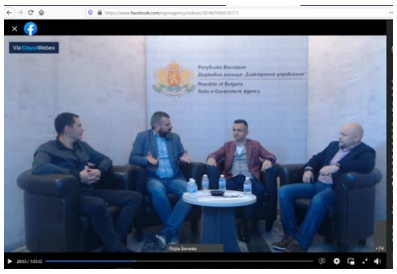
An online meeting was conducted in which ethical hackers commented on the most common cyberattacks during the Pandemic -Mariela Bakardzhieva, CERT Bulgaria; Pavel Georgiev, Co-founder and Deputy Head of the Bulgarian Association of Certified Ethical Hackers; Milcho Hekimov, Co-founder and member of the Bulgarian Association of Certified Ethical Hacker; Atanas Blagoev, member of the Bulgarian Association of Certified Ethical Hacker.



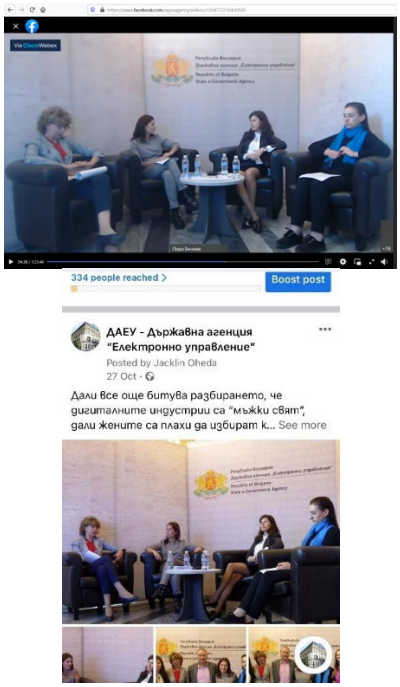
Online meeting on the topic of cybersecurity in SME. - analysis from an empirical study of cybersecurity in SMEs in Bulgaria. Experts: Boyko Takov, Executive Director Bulgarian SME Promotion Agency; Miroslav Stefanov, Expert in Network and Information Security, SEGA; Margarita Oysolova, CERT Bulgaria; Gergana Aneva, Director of Directorate at SEGA.



Online meeting on the topic: “Cybersecurity in municipalities – measures, policies and good practises”. Experts: Borislav Panayotov,IT Director - Municipality of Sofia; Miroslav Belyashki, Chief Of Staff Mayors Office at Municipality of Plovdiv; Peter Kirkov, Director Network and Information Security, SEGA; Miroslav Stefanov, Expert in Network and Information Security, SEGA

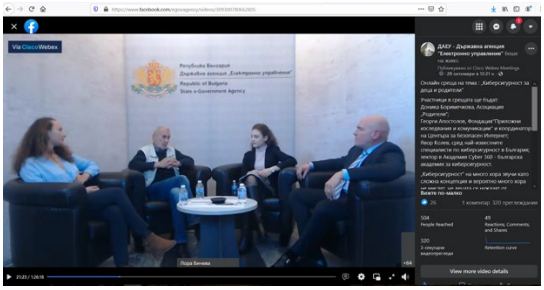


Online meeting on the topic "Women in cybersecurity“, host Alexandra Sarchadzhieva, ambassador of the campaign and experts from SEGA, Petya Marinova, Head of the Information Systems Unit at SEGA; Silvia Klicheva, Network and Information Security Expert, at the Network and Information Security Directorate, SEGA; Kalina Georgieva, Chief Legal Consultant at SEGA



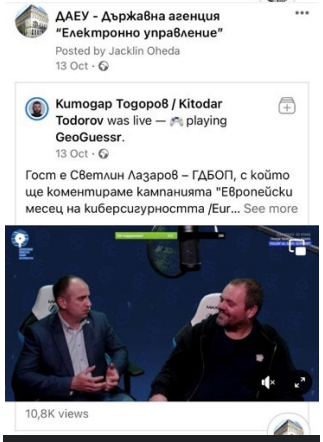
Online meeting on the topic: Cybersecurity for children and parents. Experts: Donika Borimechkova, Association “Parents”; Georgi Apostolov, Coordinator at Bulgarian Safer Internet Centre; Yavor Kolev, previous National Coordinator

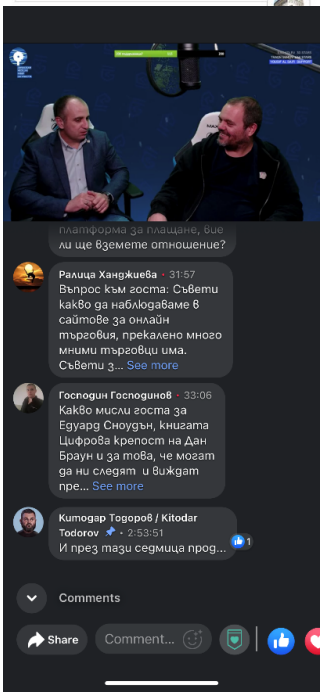
for cybersecurity and lecturer at Cyber 360 Academy - Bulgarian Academy for Cyber Security; Radina Yordanova, junior expert at SEGA.



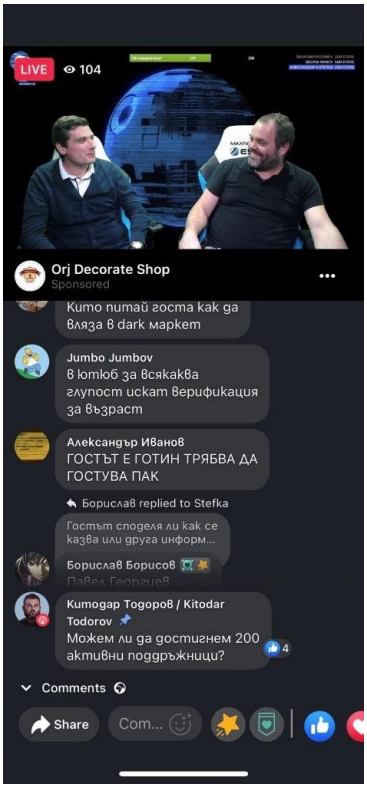
Post of Kitodar Todorov, ambassador of the ESCM-2021, announcing 2 events and his guests, that he will host dedicated to ESCM-2021 topics

Post and share of the streaming of the meeting that Kitodar Todorov, ambassador of the ESCM-2021, hosted in his social streaming channel - KitoGameing with cybersecurity expert Chief Inspector Svetlin Lazarov, Head of Digital Analyzes and Open Sources Sector at the Cyber Crime Department of the General Directorate for Fighting Organised Crime at the Ministry of Interior.

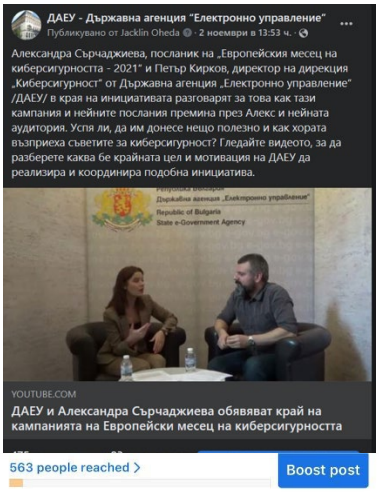




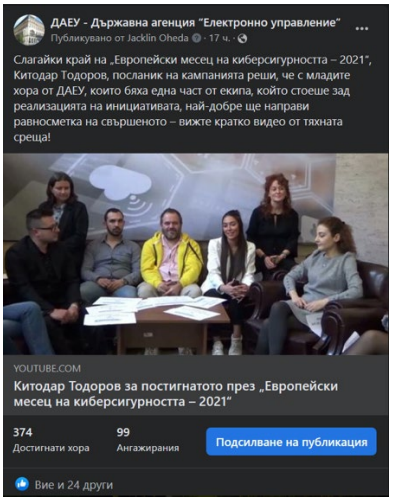
Post and share of the streaming of the meeting that Kitodar Todorov, ambassador of the ESCM-2021, hosted in his social streaming channel - KitoGameing with Pavel Georgiev, Co-founder and Deputy Head of the Bulgarian Association of Certified Ethical Hackers.



At the end of the initiative, Alexandra Sarchadzhieva, ambassador of the campaign and Peter Kirkov, Director, Network and Information Security Directorate, SEGA do a wrap up of the ESCM-2021, discussing lessons learned from the campaign and its messages and results.

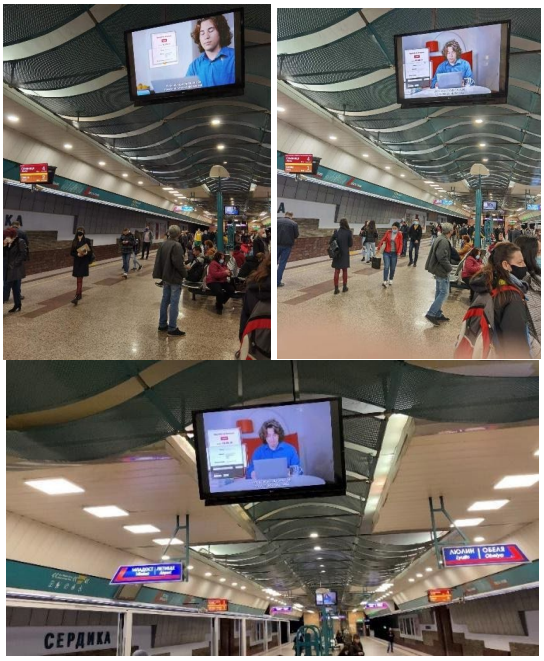


Final video, Kitodar Todorov, ambassador of the campaign and the SEGA team.



Post – end of October - don't let yourself be tricked

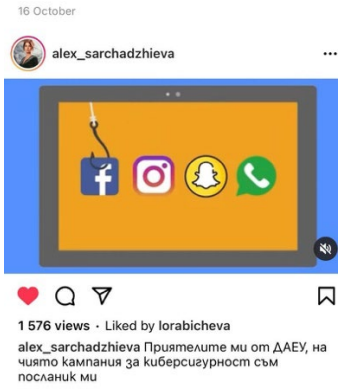
In cooperation with Sofia Metropoliten - the campaign videos were presented during entire October in all metro stations in the city of Sofia, 30 times a day.



Special practical brochure, dedicated to one of the most common cyberattacks - ransomware.

Post about how to build up habits for a secure password – change it often, don't share it, choose a strong and quality one.

Video post of Alexandra Sarchadzieva – ambassador of the ESCM-2021 about phishing



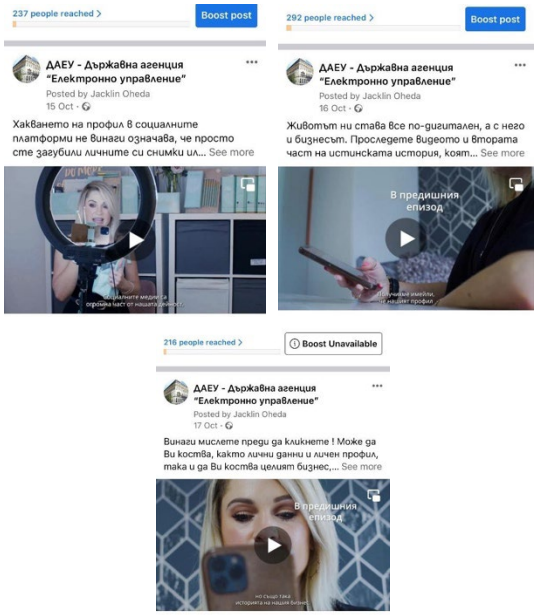
FACEBOOK POSTS:

Post of infographics

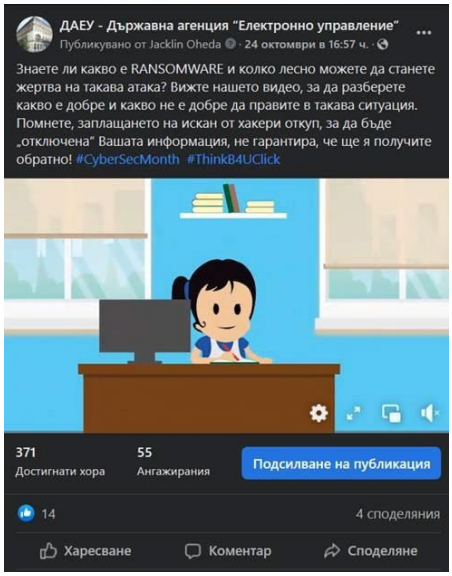
- advice for telework from home for employees
- advice for telework from home for employers

Post with infographics of ESCM-2021

Post with video of ESCM-2021

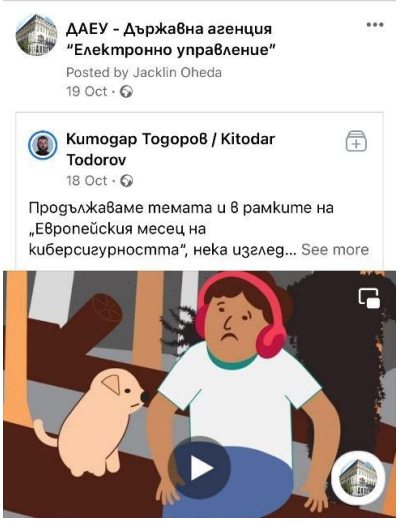


Video post on Ransomware – advice what to do and what not to do



Post with infographic

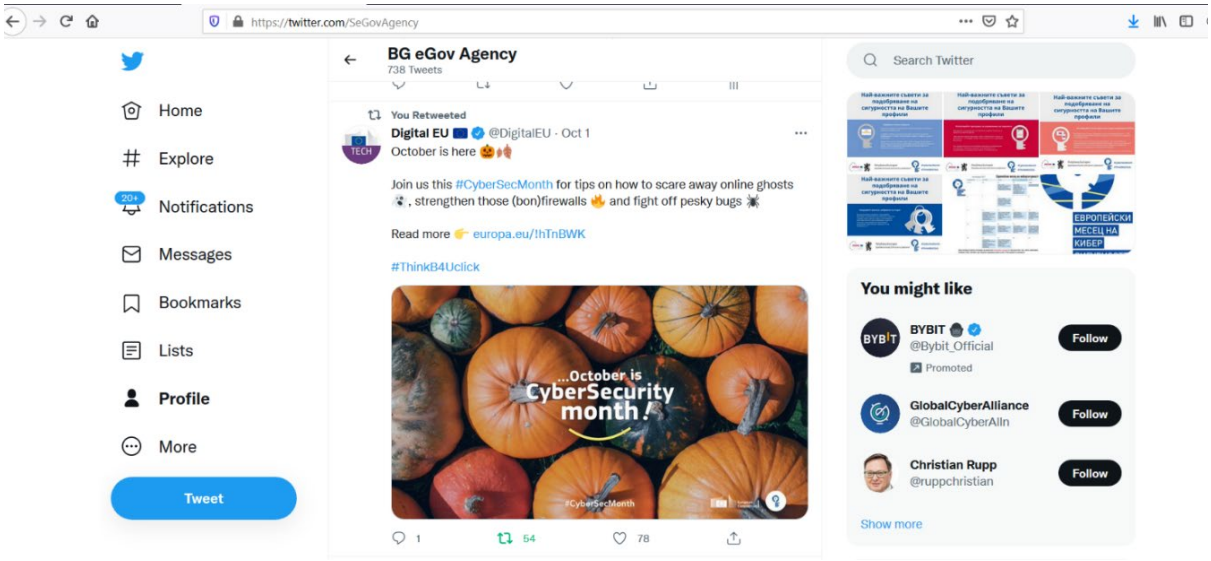
- cybersecurity for children and parents
- Video for ESCM from Kitodar Todorov, ambassador of the ESCM-2021



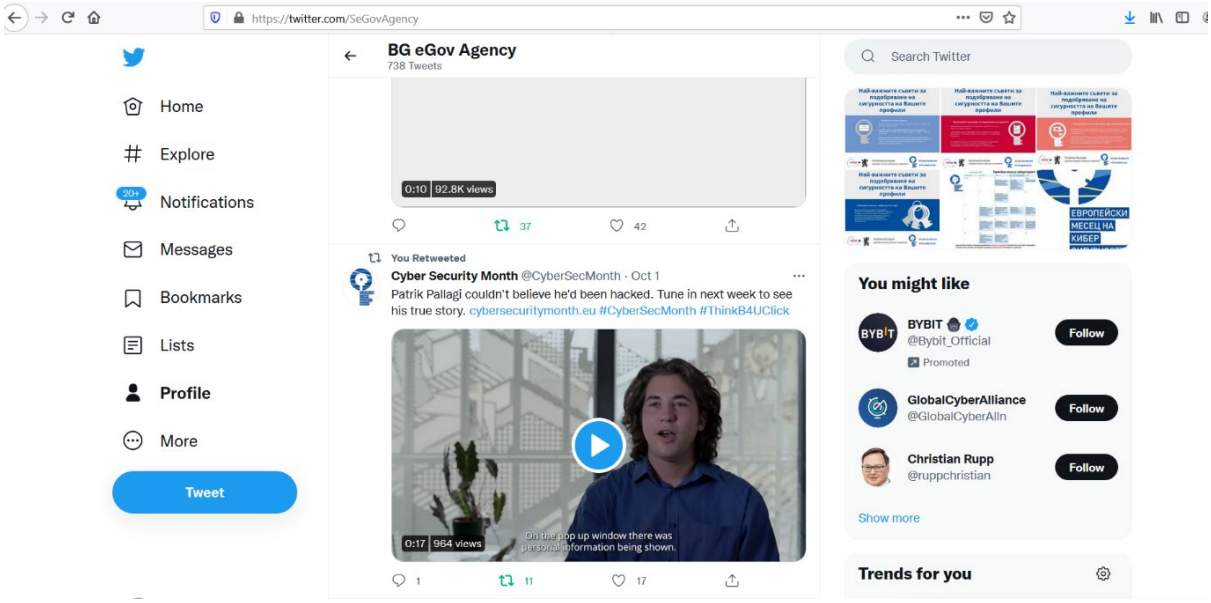
Post with infographic – cybersecurity advice for SMEs

TWITTER POSTS (RETWEETS):

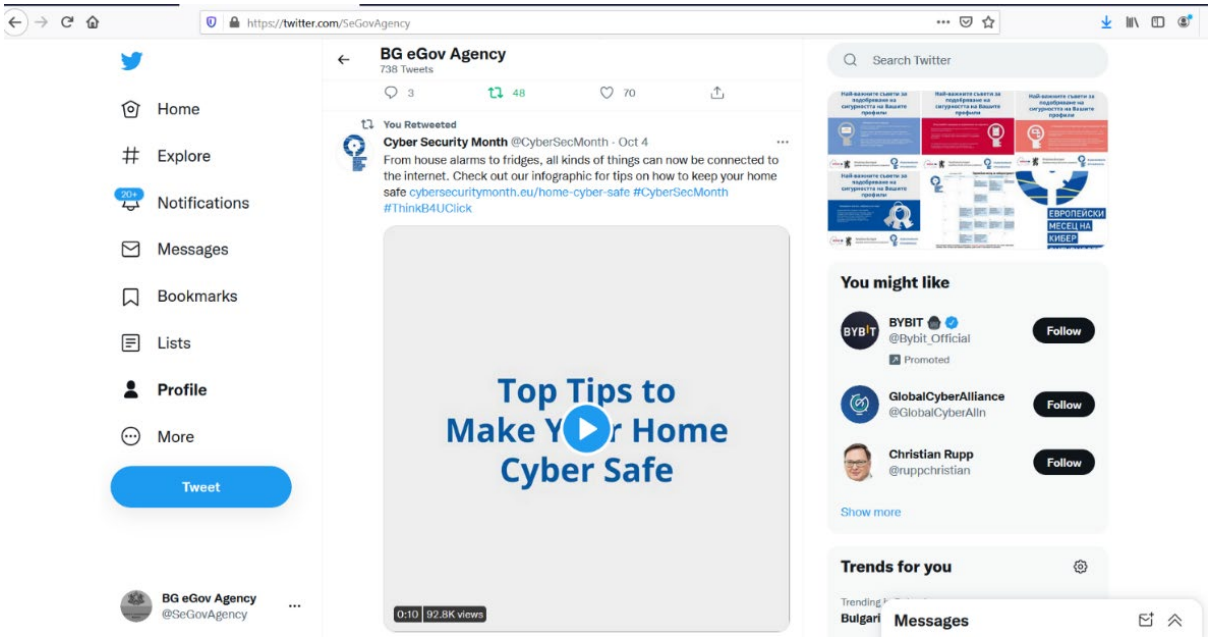
1.

2. 

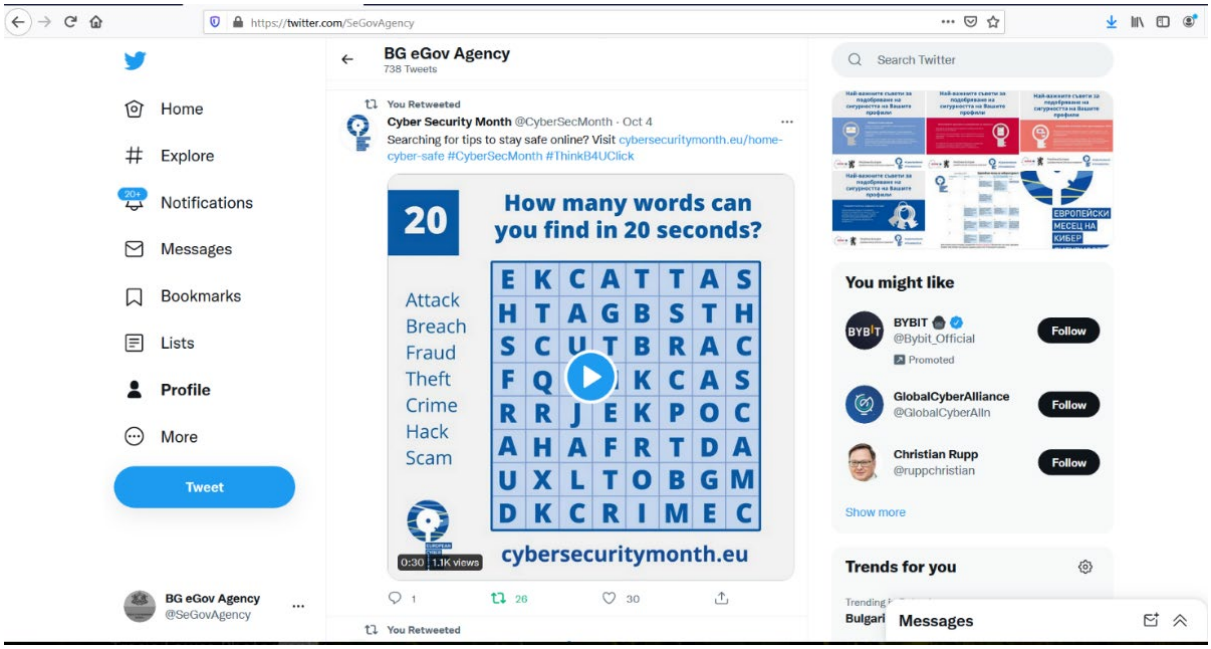
3.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
Search Twitter
0:10 92.8K views
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 1
Patrik Pallagi couldn't believe he'd been hacked. Tune in next week to see his true story. cybersecuritymonth.eu #CyberSecMonth #ThinkB4UClick
0:17 964 views
On the pop up window there was personal information being shown.
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you

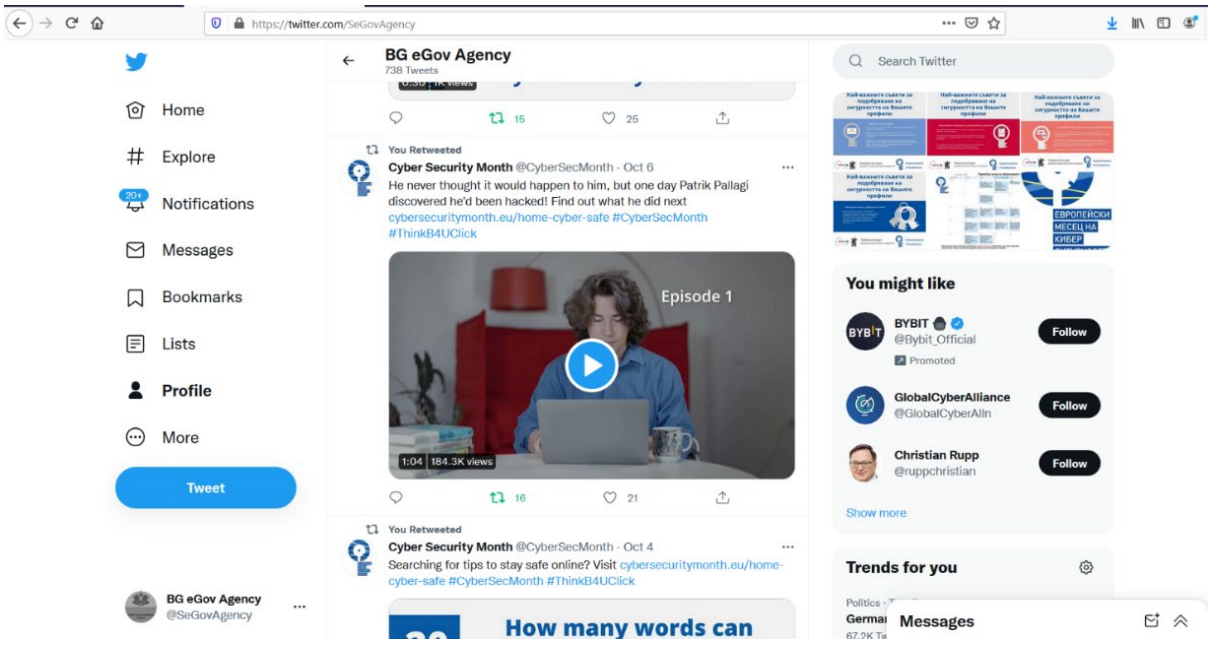
4.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
BG eGov Agency
@SeGovAgency
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 4
From house alarms to fridges, all kinds of things can now be connected to the internet. Check out our infographic for tips on how to keep your home safe cybersecuritymonth.eu/home-cyber-safe #CyberSecMonth #ThinkB4UClick
Top Tips to
Cyber Safe
0:10 92.8K views
Search Twitter
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
Messages

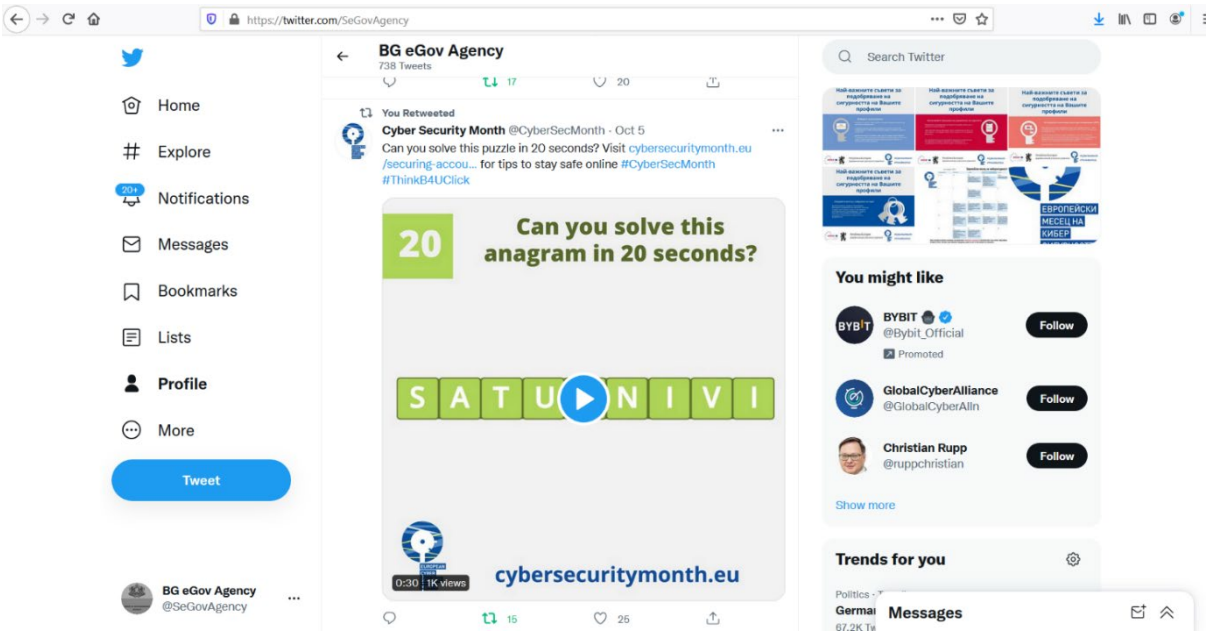
5.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Search Twitter
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 4
Searching for tips to stay safe online? Visit cybersecuritymonth.eu/home-cyber-safe #CyberSecMonth #ThinkB4UClick
20
How many words can you find in 20 seconds?
Attack
Breach
Fraud
Theft
Crime
Hack
Scam
cybersecuritymonth.eu
0:30 1.1K views
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
BG eGov Agency @SeGovAgency
Messages

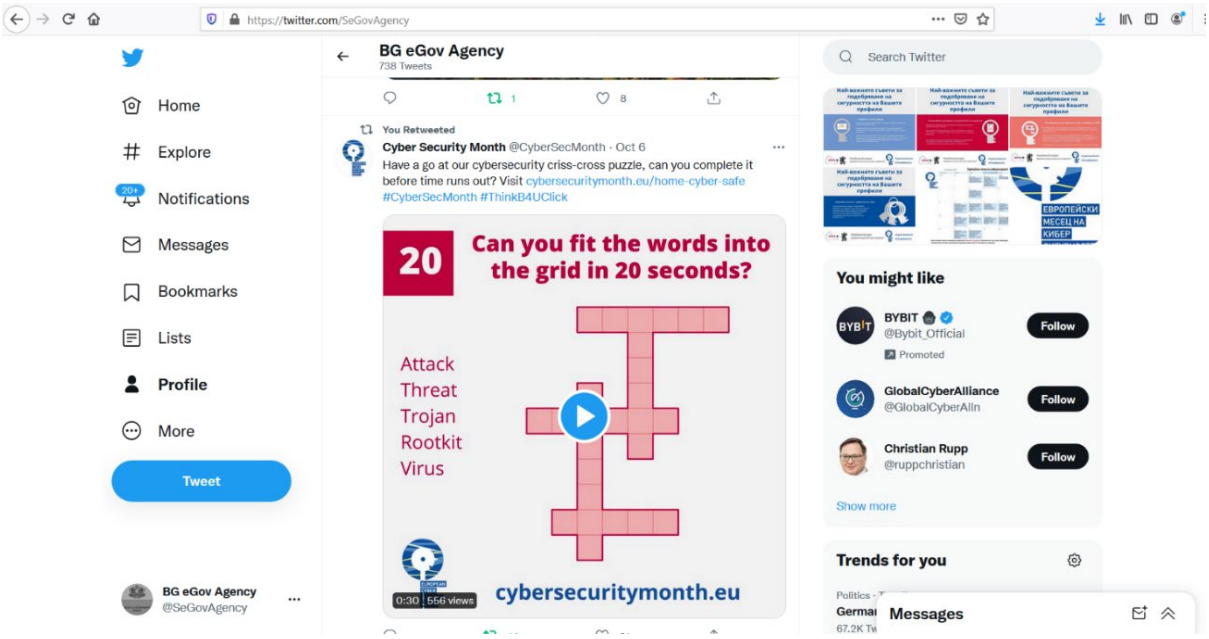
6.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Search Twitter
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 6
He never thought it would happen to him, but one day Patrik Pallagi discovered he'd been hacked! Find out what he did next cybersecuritymonth.eu/home-cyber-safe #CyberSecMonth #ThinkB4UClick
Episode 1
1:04 184.3K views
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
BG eGov Agency @SeGovAgency
Messages

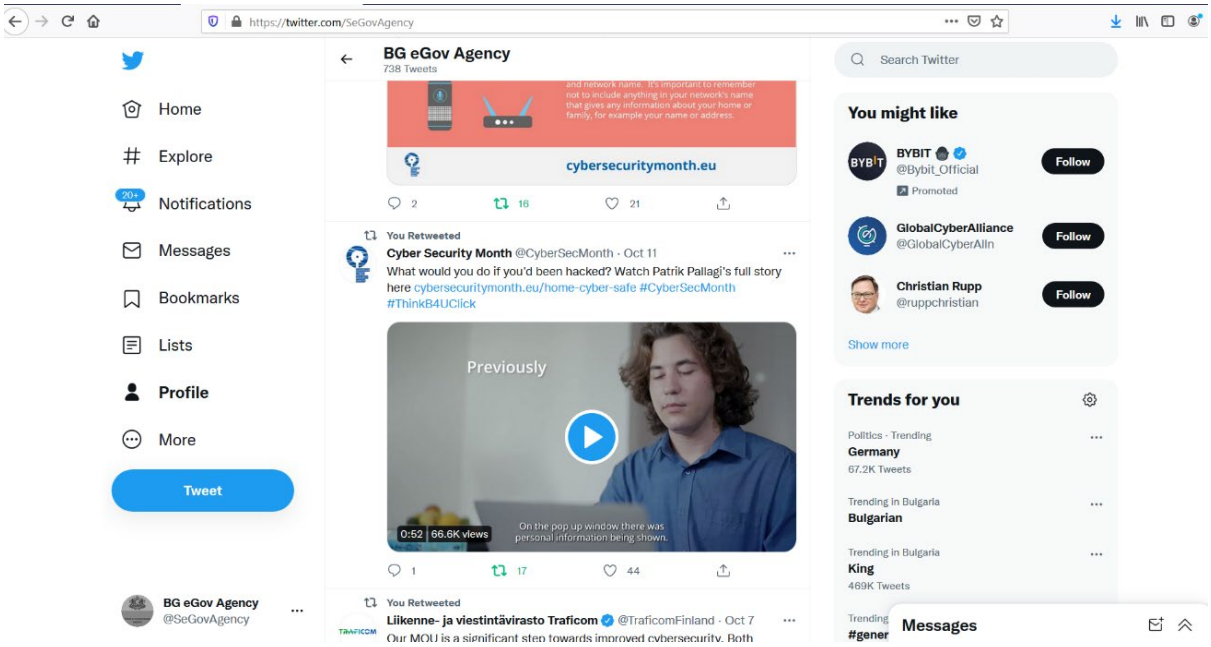
7.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
BG eGov Agency
@SeGovAgency
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 5
Can you solve this puzzle in 20 seconds? Visit cybersecurity month.eu /securing-accou... for tips to stay safe online #CyberSecMonth #ThinkB4UClick
20
Can you solve this anagram in 20 seconds?
S A T U N I V I
0:30 1K views
cybersecurity month.eu
Search Twitter
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
Messages

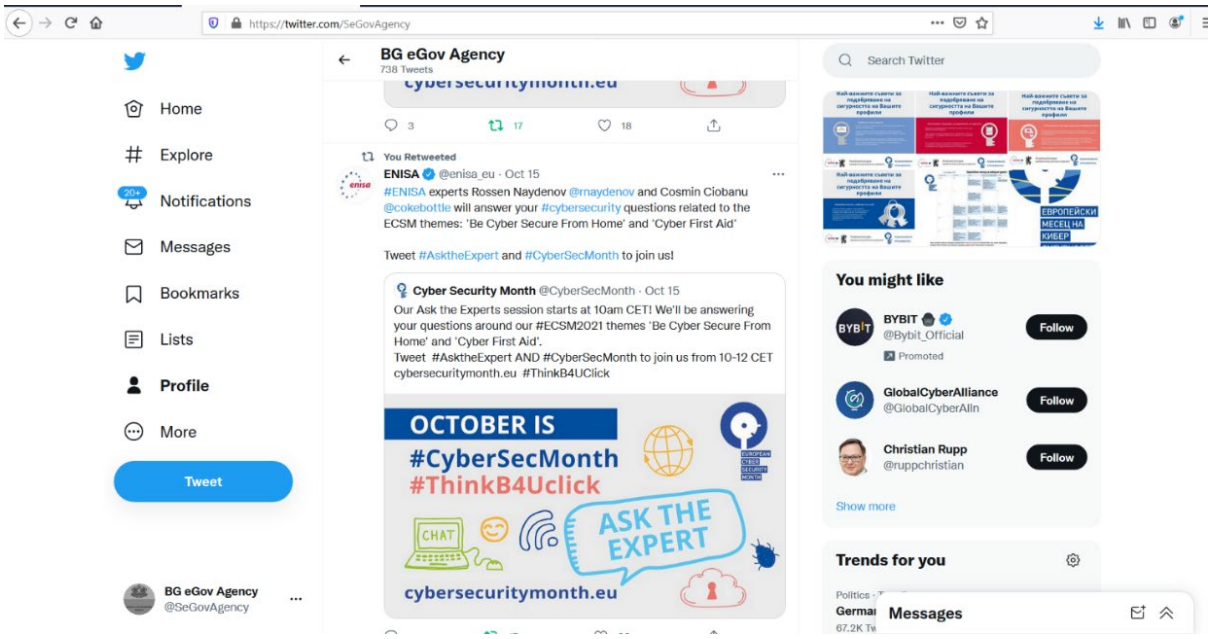
8.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
BG eGov Agency
@SeGovAgency
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 6
Have a go at our cybersecurity criss-cross puzzle, can you complete it before time runs out? Visit cybersecurity month.eu/home-cyber-safe #CyberSecMonth #ThinkB4UClick
20
Can you fit the words into the grid in 20 seconds?
Attack
Threat
Trojan
Rootkit
Virus
0:30 556 views
cybersecurity month.eu
Search Twitter
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
Messages

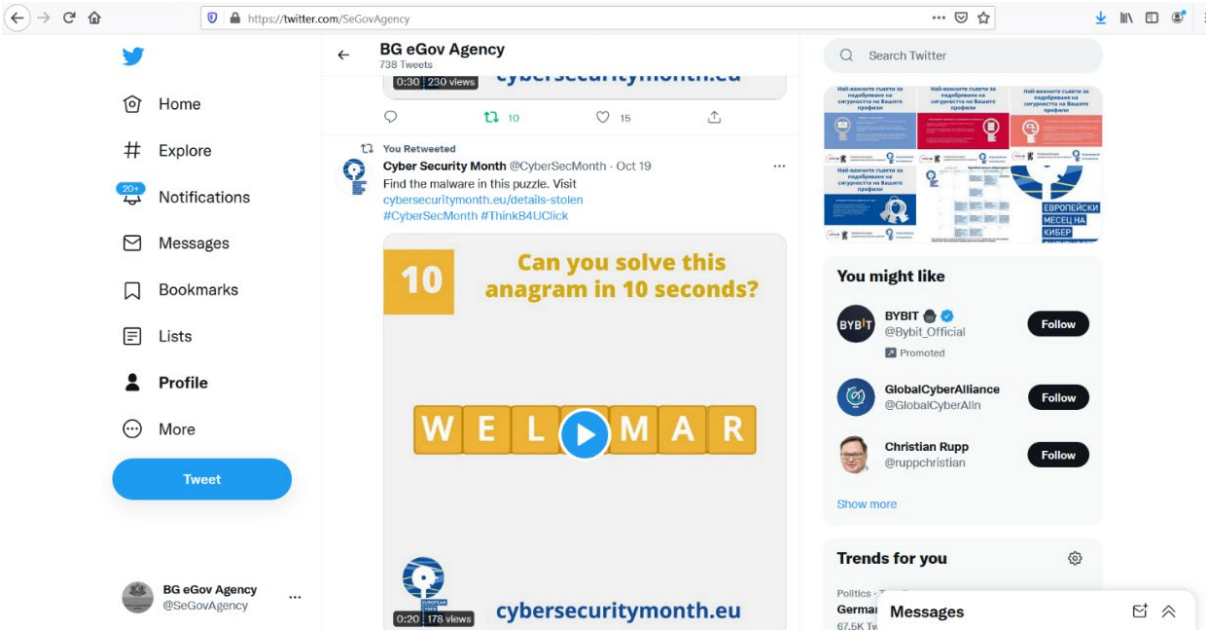
9.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Search Twitter
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
cybersecuritymonth.eu
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 11
What would you do if you'd been hacked? Watch Patrik Pallagi's full story here cybersecuritymonth.eu/home-cyber-safe #CyberSecMonth #ThinkB4UClick
Previously
0:52 66.6K views
On the pop up window there was personal information being shown.
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
Politics · Trending
Germany
67.2K Tweets
Trending in Bulgaria
Bulgarian
Trending in Bulgaria
King
469K Tweets
BG eGov Agency @SeGovAgency
You Retweeted
Liikenne- ja viestintävirasto Traficom @TraficomFinland · Oct 7
Our MOU is a significant step towards improved cybersecurity. Both
Messages

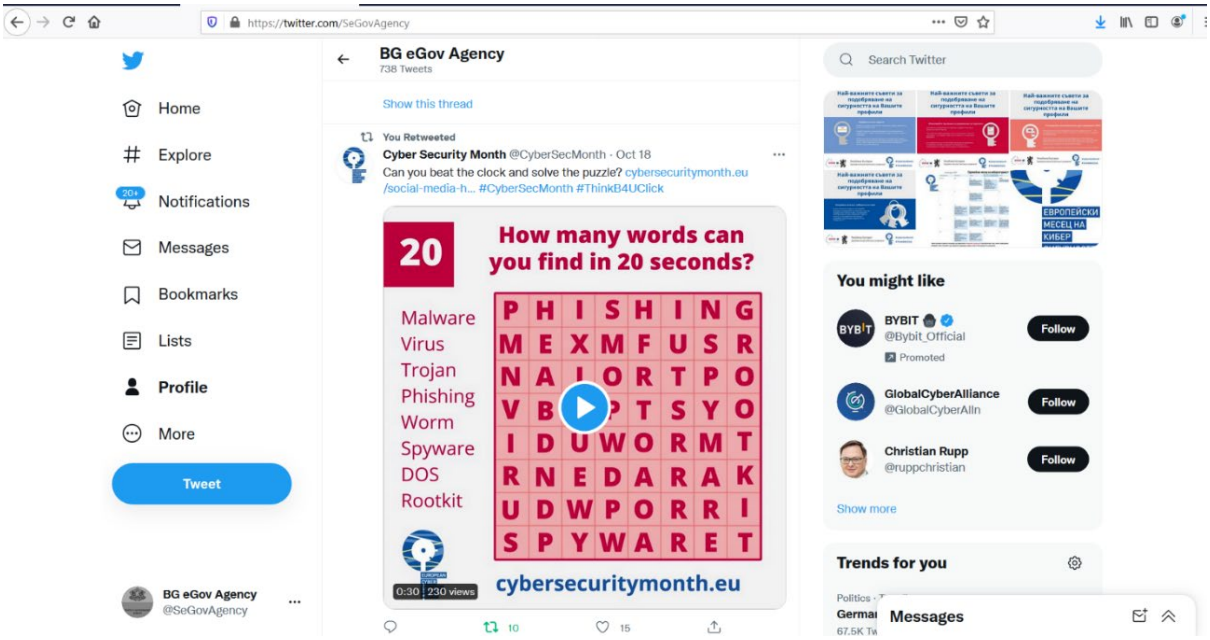
10.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Search Twitter
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
You Retweeted
ENISA @enisa_eu · Oct 15
#ENISA experts Rossen Naydenov @rnaydenov and Cosmin Ciobanu @cokebottle will answer your #cybersecurity questions related to the ECSM themes: 'Be Cyber Secure From Home' and 'Cyber First Aid'
Tweet #AsktheExpert and #CyberSecMonth to join us!
Cyber Security Month @CyberSecMonth · Oct 15
Our Ask the Experts session starts at 10am CET! We'll be answering your questions around our #ECSM2021 themes 'Be Cyber Secure From Home' and 'Cyber First Aid'.
Tweet #AsktheExpert AND #CyberSecMonth to join us from 10-12 CET
cybersecuritymonth.eu #ThinkB4UClick
OCTOBER IS
#CyberSecMonth
#ThinkB4Uclick
CHAT
ASK THE EXPERT
cybersecuritymonth.eu
ЕВРОПЕЙСКИ МЕСЕЦ НА КИБЕР
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
BG eGov Agency @SeGovAgency
Messages

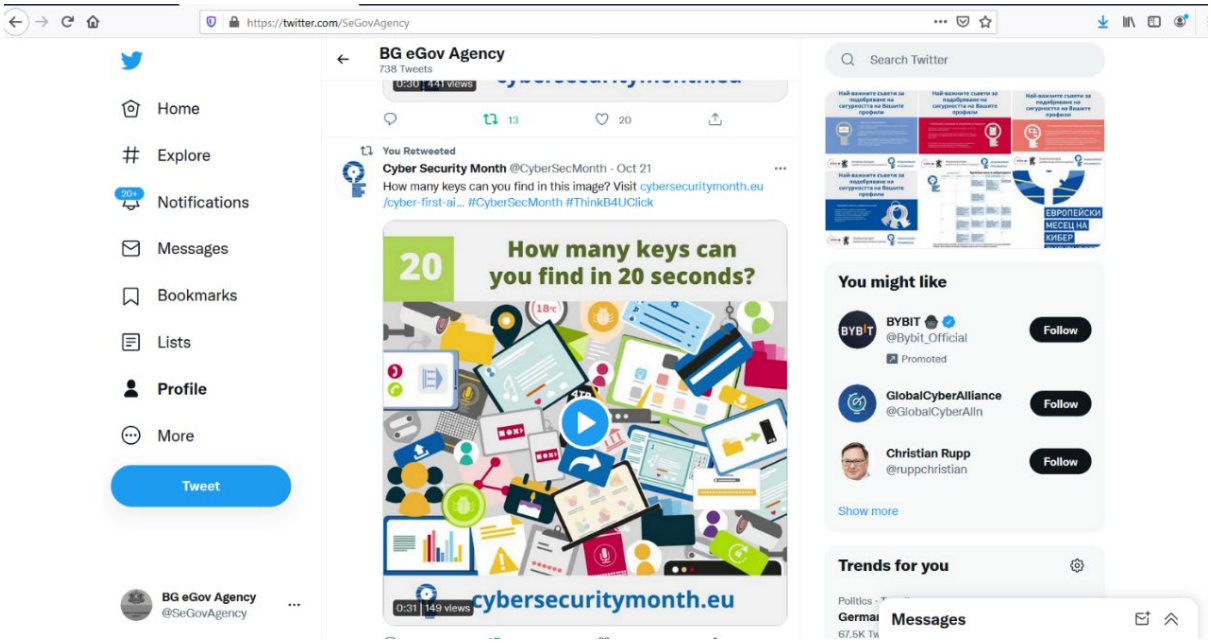
11.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
BG eGov Agency
@SeGovAgency
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 19
Find the malware in this puzzle. Visit
cybersecuritymonth.eu/details-stolen
#CyberSecMonth #ThinkB4UClick
10
Can you solve this anagram in 10 seconds?
W E L M A R
0:20 178 views
cybersecuritymonth.eu
Search Twitter
You might like
BYBIT
@Bybit_Official
Promoted
Follow
GlobalCyberAlliance
@GlobalCyberAlln
Follow
Christian Rupp
@ruppchristian
Follow
Show more
Trends for you
Messages

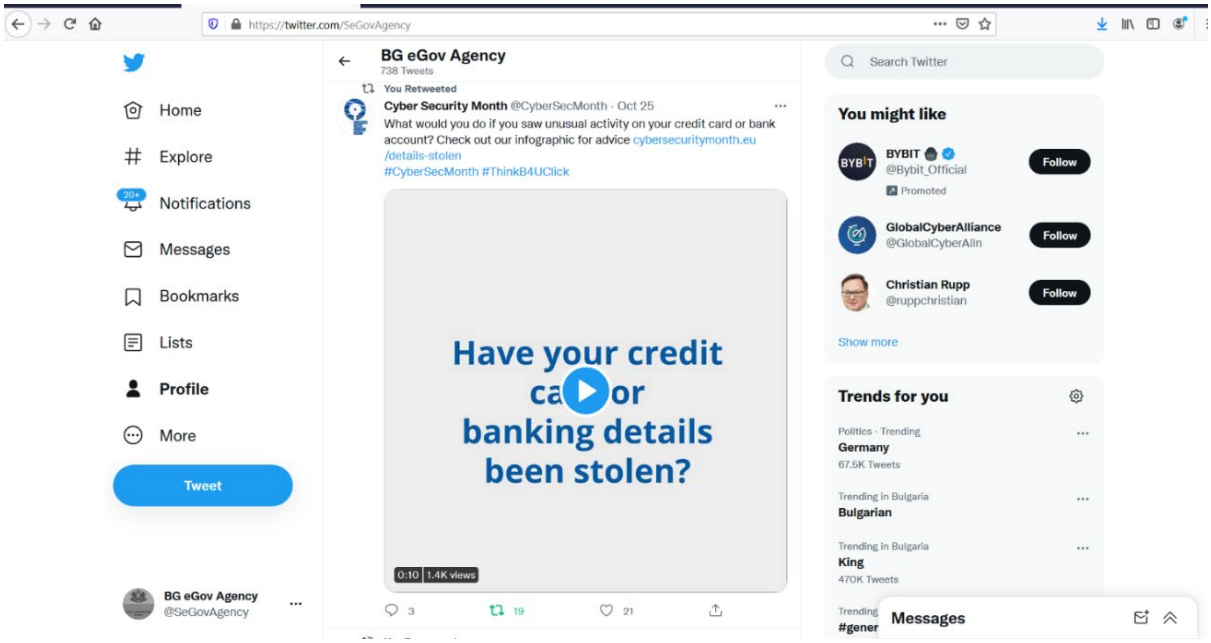
12.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Show this thread
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
BG eGov Agency
@SeGovAgency
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 18
Can you beat the clock and solve the puzzle? cybersecuritymonth.eu
/social-media-h... #CyberSecMonth #ThinkB4UClick
20
How many words can you find in 20 seconds?
Malware
Virus
Trojan
Phishing
Worm
Spyware
DOS
Rootkit
P H I S H I N G
M E X M F U S R
N A I O R T P O
V B P T S Y O
I D U W O R M T
R N E D A R A K
U D W P O R R I
S P Y W A R E T
0:30 230 views
cybersecuritymonth.eu
Search Twitter
You might like
BYBIT
@Bybit_Official
Promoted
Follow
GlobalCyberAlliance
@GlobalCyberAlln
Follow
Christian Rupp
@ruppchristian
Follow
Show more
Trends for you
Messages

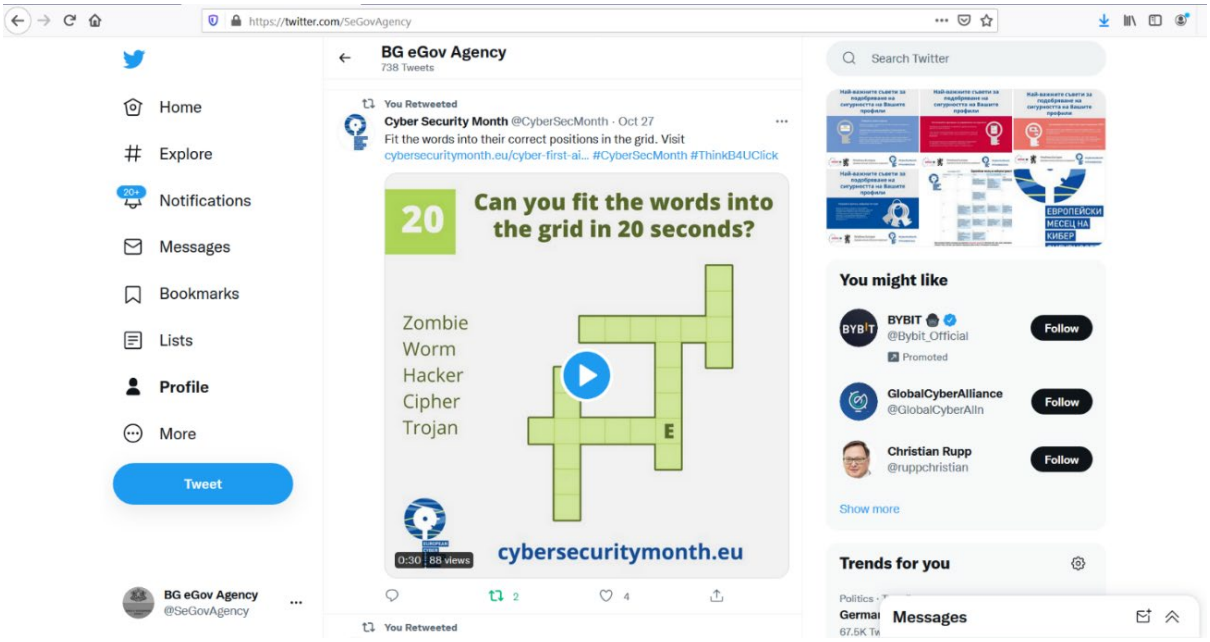
13.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Search Twitter
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 21
How many keys can you find in this image? Visit cybersecuritymonth.eu /cyber-first-ai... #CyberSecMonth #ThinkB4UClick
20
How many keys can you find in 20 seconds?
0:31 149 views
cybersecuritymonth.eu
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
Messages
BG eGov Agency @SeGovAgency

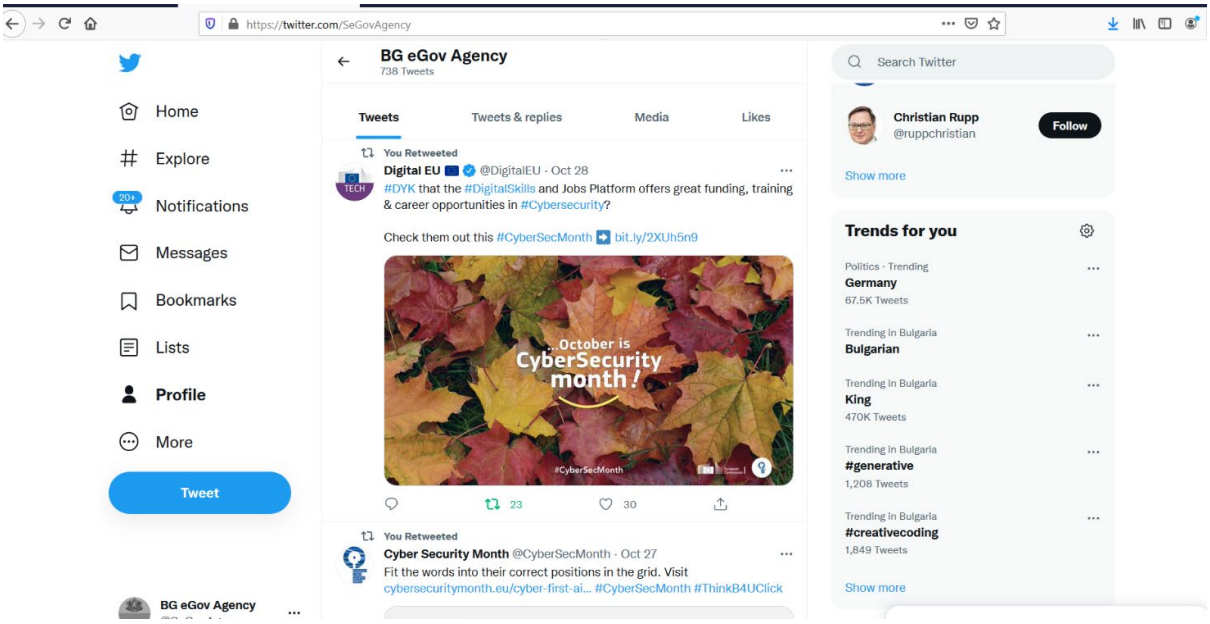
14.


https://twitter.com/SeGovAgency
BG eGov Agency
738 Tweets
Search Twitter
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
You Retweeted
Cyber Security Month @CyberSecMonth · Oct 25
What would you do if you saw unusual activity on your credit card or bank account? Check out our infographic for advice cybersecuritymonth.eu /details-stolen #CyberSecMonth #ThinkB4UClick
Have your credit ca or banking details been stolen?
0:10 1.4K views
You might like
BYBIT @Bybit_Official Promoted Follow
GlobalCyberAlliance @GlobalCyberAlln Follow
Christian Rupp @ruppchristian Follow
Show more
Trends for you
Politics · Trending Germany 67.5K Tweets
Trending in Bulgaria Bulgarian
Trending in Bulgaria King 470K Tweets
Messages
BG eGov Agency @SeGovAgency

15.

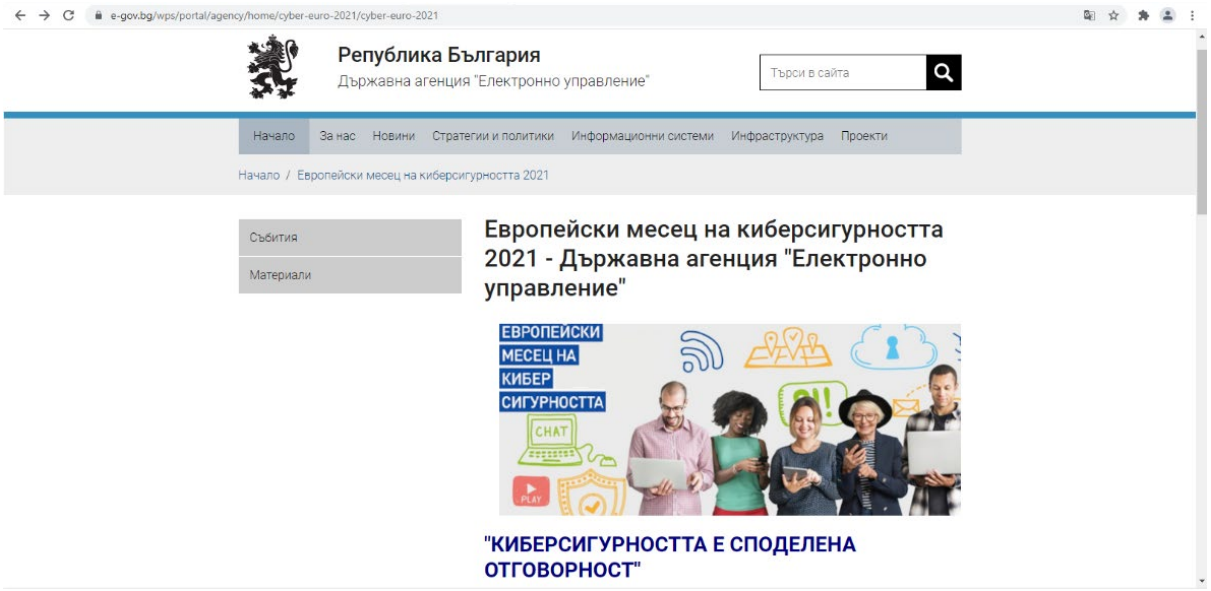


16.

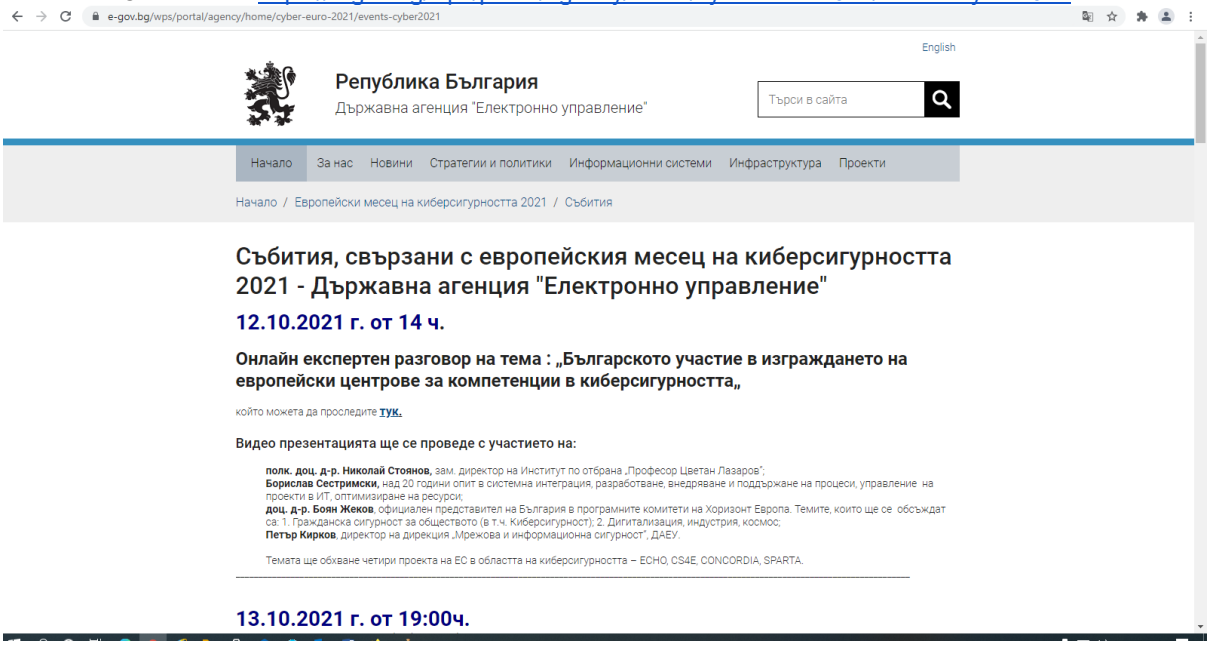


WEBSITE – SECTION DEDICATED TO THE ESCM-2021

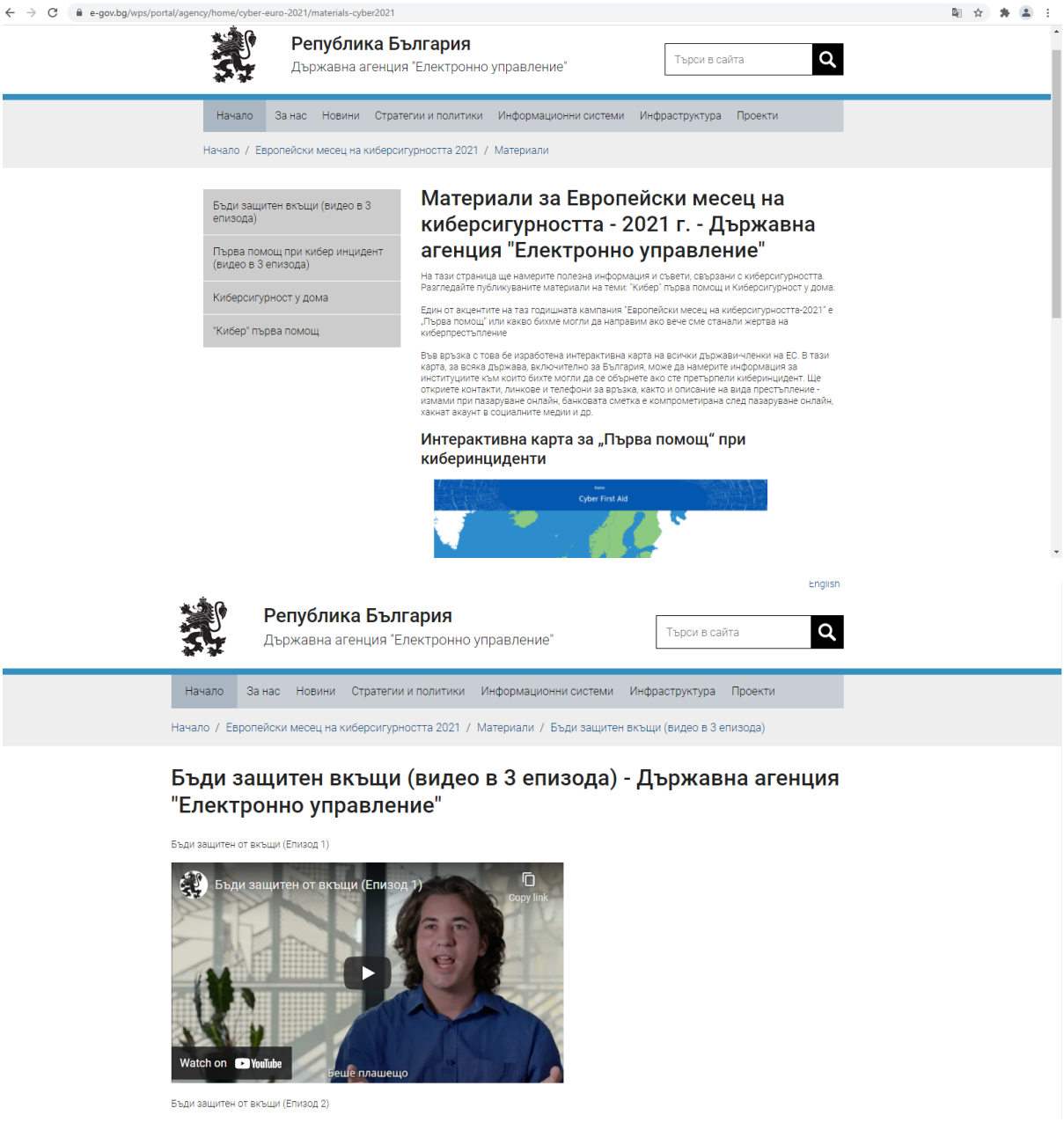
https://e-gov.bg/wps/portal/agency/home/cyber-euro-2021



EVENTS - CALENDAR https://e-gov.bg/wps/portal/agency/home/cyber-euro-2021/events-cyber2021



MATERIALS TO DOWNLOAD https://e-gov.bg/wps/portal/agency/home/cyber-euro-2021/materials-cyber2021

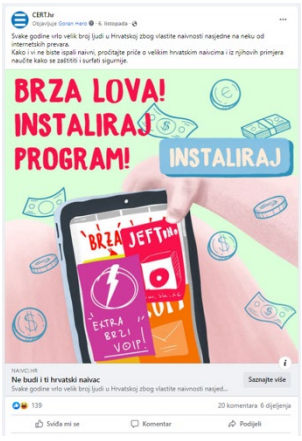


Croatia

The Croatian National CERT had several activities during the European Cybersecurity Month and one of them was national cybersecurity awareness raising campaign Great Croatian Naives with two short video spots:
Ivana downloading malware in her quest for easy money and
Daniel losing money in search for love of his life

Videos were broadcasted on Croatian National Television and are available on YouTube channel of National CERT.

There are two social media posts related to topics of catphishing / scam and malware distribution:



The landing page for social media posts is https://naivci.hr/#Aktivnosti where interactive content is available for the general public. There are ten different activities in the form of games and quizzes. Covered topics are: Cybersecurity fun facts, memory games on cybersecurity, key terms like digital footprint, backup, passphrase, netiquette, CSIRT, cyber hygiene, and games on cybersecurity threats such as malware, phishing, social engineering, spam, data breach, hacker. There are also tests on phishing e-mail and cyber hygiene.

Topics
Topics covered during ECSM 2021 were digital footprint, cyber hygiene, netiquette, first aid for cybersecurity victims, safe remote work and education.

Highlights of ECSM 2021 were:

- **Hacknite 2.0** - second edition of 48-hour CTF competition for highschool students, this year we had 51 teams with 155 players (https://www.cert.hr/prijavite-se-na-natjecanje-hacknite-2-0/ , https://www.cert.hr/pobjednici-hacknite-hr-2-0-upoznajmo-tim-gospoda/), its goal was to promote cybersecurity among teenagers, by applying technical knowledge in cryptography, malware analysis, steganography etc.
- **Panel discussion** "How susceptible are we to manipulation?" - it took place in early November, people participated from the Faculty of Law, Croatian Banking Association, private cybersecurity firm Diverto, Ministry of the Interior and Croatian National CERT. The topics of the discussion were social engineering, cyber hygiene and raising security awareness.
    - Invitation: https://www.cert.hr/panel-rasprava-koliko-smo-podlozni-manipulaciji/
    - Conclusions: https://www.cert.hr/odrzana-panel-rasprava-koliko-smo-podlozni-manipulaciji/
- Promo educational materials:
    - https://www.cert.hr/savjeti-za-zastitu-na-internetu/
    - https://www.cert.hr/sto-uciniti-ako-nam-netko-preuzme-virtualni-identitet/
    - https://www.cert.hr/savjeti-za-zastitu-racuna-na-drustvenim-mrezama/
    - https://www.cert.hr/sto-uciniti-ako-su-vam-ukradeni-podaci-o-kreditnoj-kartici-ili-bankovni-podaci/

Cyprus

Exposition
In the fast-growing technological world that we live in today, everyone, regardless of their age, has at least one interaction with technology and the internet a day. That may be for reading the news, reading an email, communicating with family, ordering food, purchasing goods and so on.
It is of a great importance to educate as many people as possible and make them aware of the dangers that technology and the internet hold for them even while doing the simplest tasks, like browsing the internet. On a small island like Cyprus, there was a need to relay this message to all citizens and make them aware of the different ways they can protect themselves; what to look out for and what to avoid, especially nowadays when the pandemic is being used as the main theme for phishing campaigns.

Problem
In order to make sure that we reached as many people as possible we needed to involve as many institutions as possible; the academic community; the private sector; the public sector; the press; and use any social media available to the organisation to promote all the material and events surrounding cybersecurity month.

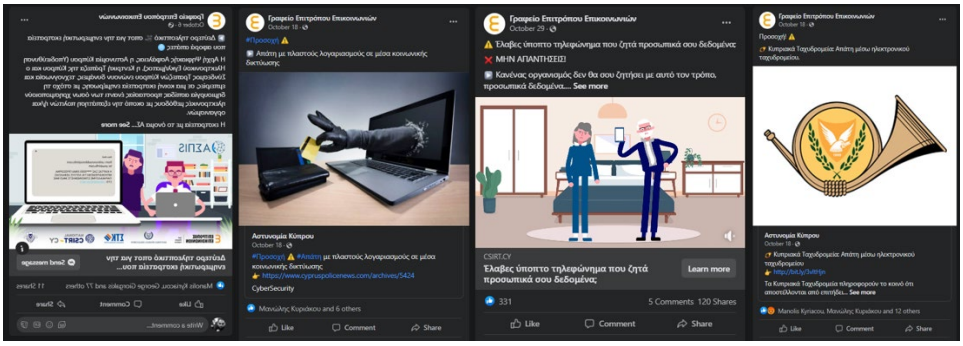
Resolution
Alongside the material created by the ECSM, we arranged events with the academic community which allowed us to reach as many students as possible and we involved private sector businesses in order to involve as many private sector employees as possible. Furthermore, we posted the infographics, videos and material made available to us using the social media channels of the organisation, this allowed us to reach as many people as possible regardless of age group.

Result
Using the material and events of the 2021 ECSM campaign we managed to reach many more people than during other months or in previous years. This can be verified by the influx of reports we got from citizens regarding suspicious emails, suspicious links and general enquiries regarding cybersecurity since the campaign ran.

Conclusion
It is clear from campaigns like ECSM and other cybersecurity related awareness campaigns that the safety of cyberspace for any member state starts with its citizens.

Campaign Visuals
Facebook post regarding the start of ECSM 2021

Posts regarding the campaign ASPIS that ran during ESCM 2021 regarding Phishing Awareness with main theme Banking Phishing and Post Office Phishing.



All events held during Cybersecurity Month 2021

21 OCT 20
21 OCT 20

Cyprus

CYBER.CERIDES Launch Event

Cybersecurity has risen to the top of political agendas. Cyber-attacks create huge damage for companies and organizations. It is important for governments, businesses and academia to stay at the forefront of these developments through cyber-risk assessment. CYBER.CERIDES aims to provide world-class expertise i…

All users

---

24 SEP 21
24 OCT 21

Cyprus

ΑΣΠΙΣ – ΕΚΣΤΡΑΤΕΙΑ ΕΝΗΜΕΡΩΣΗΣ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Τα ηλεκτρονικά εγκλήματα ή απάτες αποτελούν ουσιαστικά τους τρόπους με τους οποίους κάποιοι κακόβουλα επιδιώκουν να αποκομίσουν χρήματα από ανυποψίαστους ιδιώτες ή επιχειρήσεις. Πολλοί πέφτουν σε αυτή την παγίδα, αφού η βασική τακτική που χρησιμοποιείται είναι η συλλογή πληροφοριών μέσω μηχανισμών που λειτουργούν από…

All users

---

22 OCT 21
22 OCT 21

Cyprus

Entry points & career opportunities in cybersecurity

The purpose of this seminar is to highlight the multidisciplinary nature of cybersecurity and inform young people, parents and career advisors about entry points and career opportunities in cybersecurity. Additionally, the seminar will highlight the cybersecurity related knowledge and skills that young people shou…

Young users

---

27 OCT 21
27 OCT 21

Cyprus

Awareness raising activities for seniors

Seniors are a significant segment of the population. They are engaged into social media, online shopping, and other activities that the pandemic and the digitisation of the society in general imposed to them. The unawareness of users about threats that they can face in cyberspace, can cause the successful…

Senior users

---

29 OCT 21
29 OCT 21

Cyprus

Cybersecurity awareness exercises in cyber ranges for critical infrastructures

The scope of this presentation and workshop/demonstration activity is to present and demonstrate the dangers of social engineering and the typical techniques used to horizontally penetrate critical infrastructures. Workshop / demonstration will be carried out over Open University of Cyprus (Cybersecurity &…

Business users

---

30 OCT 21
30 OCT 21

Cyprus

Cyberbullying Youth event

Center for Social Innovation – CSI Cyprus is proud to invite you to the Youth Event held for the purposes of the Erasmus+ project 'Initiatives against Cyberbullying and Hate in Social Media', in which our organization is a coordinator! The Youth Event will bring together students, teachers, youth workers, trainers, youth…

All users

---

17 NOV 21
17 NOV 21

Cyprus

Awareness raising activities for SMEs

SMEs have been at the center of cyberattacks in particular during the last 1.5 years, due to the digitization they were forced to undergo because of the pandemic. This seminar attempts to shed light on the most important concepts and definitions with regards to cybersecurity, the various attacks, what is a digit…

Business users

Czech Republic

Exposition
Digital technologies are an integral part of our lives. Digital technologies allow us to do things that were unthinkable just ten years ago and they give us access to an enormous amount of knowledge. The coronavirus pandemic has accelerated this digital transformation, with a sudden and large-scale move to teleworking; the use of digital services in hospitals, laboratories and government services; and the explosion in online schooling. However this trend brings with it not only an increase in the number of end users, but also the threats to which they are exposed.

Problem
The National Cyber Security Strategy of the Czech Republic 2021 – 2025 defines poor digital hygiene as a key issue. Cybersecurity tools on their own are not sufficient protection against today's many threats. There is a need to integrate cybersecurity at all levels of the education system and to support educational activities in the field of cybersecurity. Education is one of the most important investments a country can make in its future.

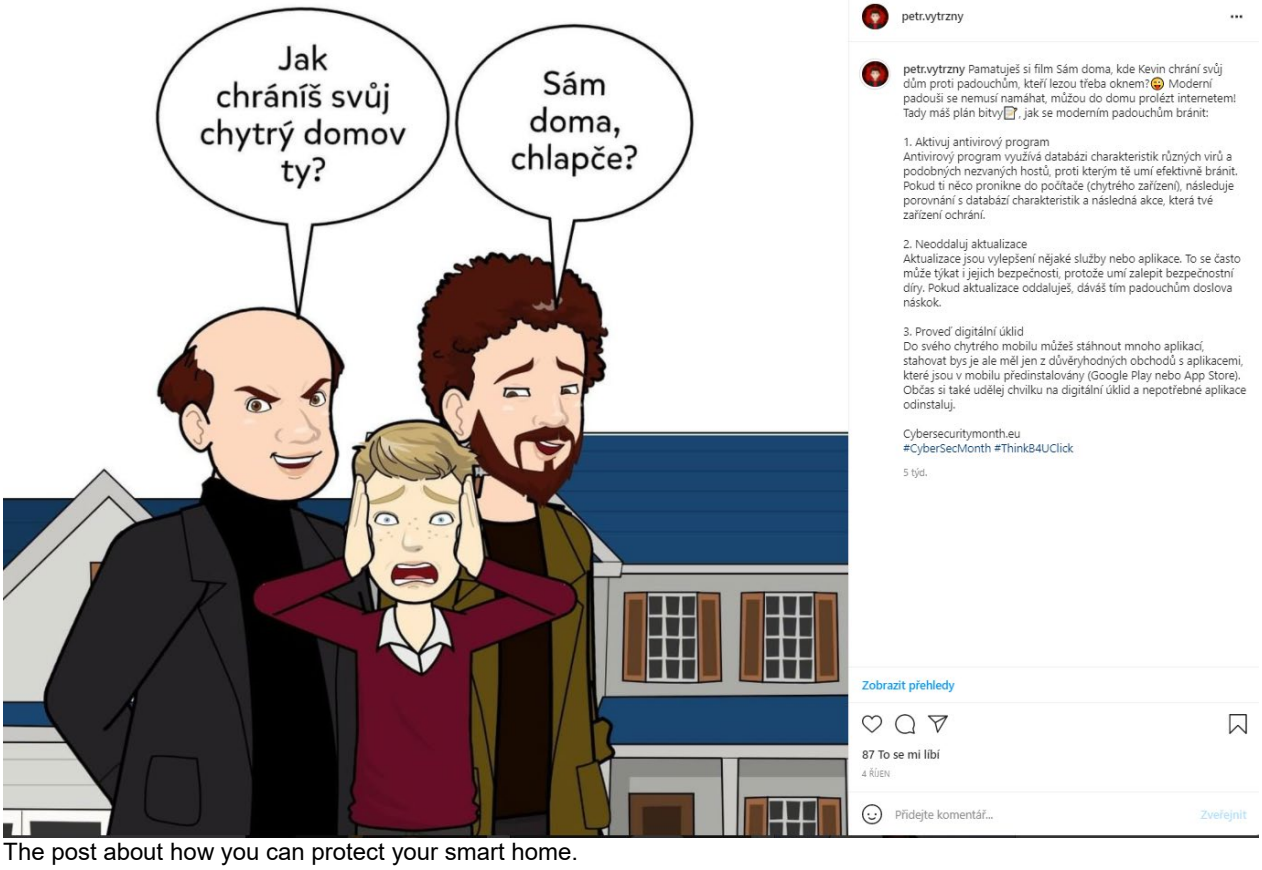
Resolution
The National Cyber and Information Security Agency (NÚKIB) is the central administrative body for cybersecurity, including the protection of classified information in information and communication systems and cryptographic protection. We have been providing education to diverse target groups for a long time. One of these groups are children. We decided to focus this year´s campaign on this group. Children over the age of 13 can follow our education Instagram @petr.vytrzny. Petr Výtržný is a comic-book character who shares fun facts from the world of digital technology and cybersecurity. We decided to use this social media to share the ECSM campaign. We prepared a series of posts based on ECSM´s materials. The most important thing was to prepare eye-catching pictures.

Result
Raising awareness of cybersecurity issues is our long-term goal. There are many ways to reach this goal. Today, children spend a lot of time on social media channels. Many children ask for advice there and because of this, social media channels are a great tool for informal education. The ECSM campaign provided a lot of tips to end users. Part of the campaign was topics we focus less on, for example, risky e-shops. Thanks to this we were able to provide followers with new content. We also challenged followers to action. ECSM posts have on average more likes than others. The campaign also supported an important aspect of cybersecurity - international cooperation.

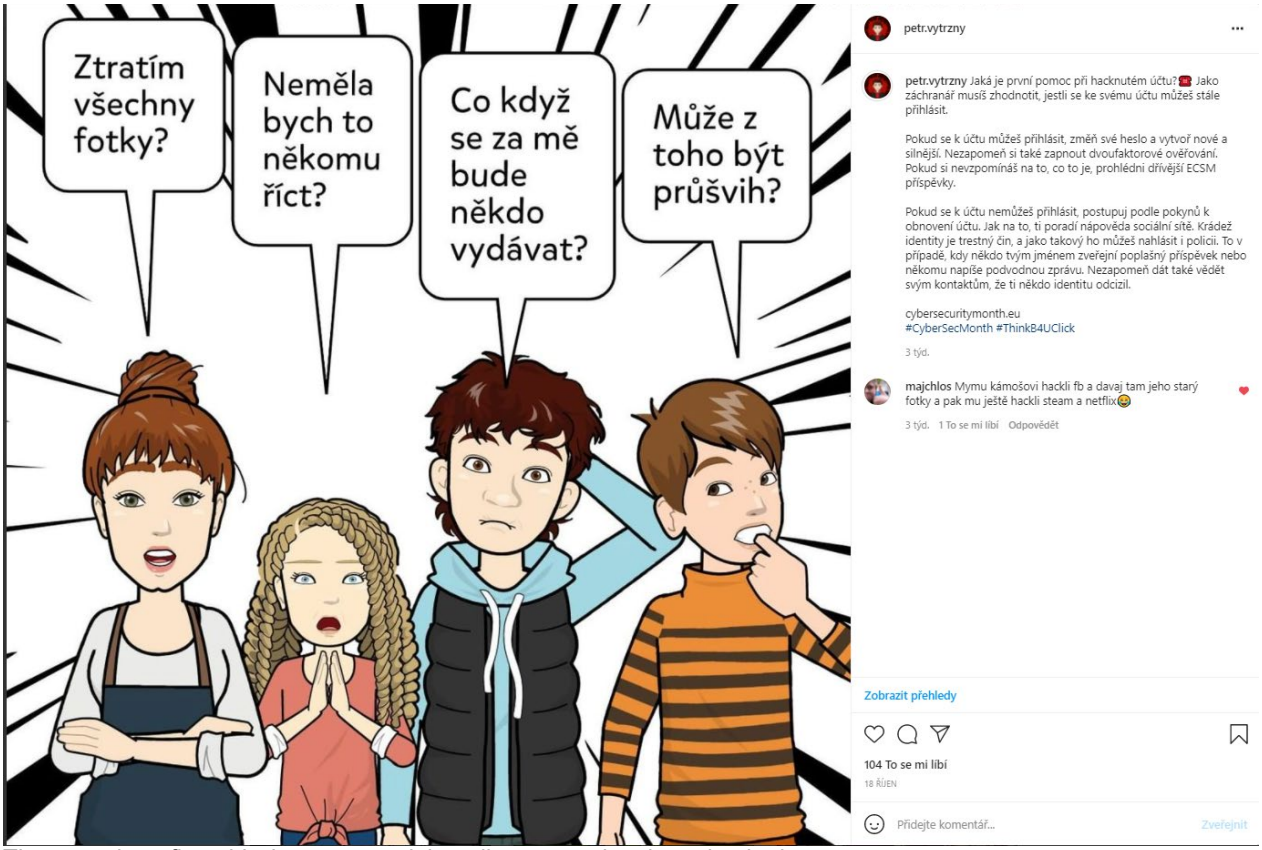
Conclusion
Social media helps us to stay in touch with children. It is important to think about what information you want to share and what is the best method. It's getting harder and harder to get the attention of followers. Therefore, information should be short. It is also important to complete the posts with eye-catching pictures. Children, especially, attach great importance to the visual side of communication. It is our message and challenge for next year´s campaign too.

Campaign Visuals

The post about how children can provide support to grandparents with their social media.



The post about how you can protect your smart home.



The post about first aid when your social media account has been hacked.

Estonia

This year the ECSM coincided with Estonian local municipalities elections on October 18th. Since we here in Estonia are able to vote online (digital i-voting), our organisation decided to focus on election security and what voters themselves can do to keep themselves safe when voting online. This meant that we took part in the European cybersecurity month campaign by distributing the two videos and infographics on our Facebook page and retweeting ECSM materials on our Twitter account. No additional ECSM-related events were organised by us, but everywhere we talked about election cybersecurity, we emphasised that October is the cybersecurity month and this is why we call on all voters to be safe online when they vote.

Next year we will definitely work more towards engaging with other organisations and put up some events to celebrate ECSM. All the materials were useful and great and we were able to share those on our social media to remind people that ENISA is still promoting this all around Europe with our partners in other member states.

Finland

Exposition

In Finland, NCSC-FI, ran the ECSM campaign on social media and on our website. The website, materials and social media posts were published in Finnish, Swedish and English. Apart from two short videos and a few online articles we used materials produced by ENISA/ECSM only.

Website: https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-European-cyber-security-month/

Twitter: https://twitter.com/CERTFI

Facebook: https://www.facebook.com/NCSC.FI/

We published the ECSM cyber tips and advice (infographics and videos) on our website and shared them via our social media channels in Twitter and Facebook. We uploaded the videos and published them on YouTube. The main cyber issues or needs in Finland are mainly the same as anywhere else in Europe. From our point of view phishing is the biggest cyber risk that the average Finnish citizen faces.

Problem

At the moment phishing and stealing of online banking credentials cause the main problems among citizens. People have lost millions of euros to cyber criminals. Criminals use fraudulent e-mails and text messages. Senior citizens aged 70 -79 are most vulnerable target group for these scams.

https://www.kyberturvallisuuskeskus.fi/en/fraudsters-stealing-banking-credentials-fake-my-kanta-pages-and-suomifi-messages

During the fall of 2021 NCSC-FI noticed that incident reports concerning hacked social media accounts had increased.

Resolution

ECSM themes Being cyber secure from home, the Cyber First Aid Kit, and the materials produced, covered our needs very well. Our ECSM campaign's top 2 tweets concerned the topics Has your social media account been hacked? and Have your credit card or banking details been stolen?

Result

We did our best with the materials provided and the resources we had. However the followers of NCSC-FI's social media channels are mostly cyber aware men, not for example the elderly or women aged 18 to 65 who are not cyber orientated. These are the people who need cyber aid the most and the ones we should reach.

Facebook and Instagram would work best if we had paid campaign posts on Facebook or a specific campaign with social media influencers on Instagram.

The best thing about ECSM campaign is that it brings more materials - tips and advice for everyday cyber life - to our website. Those materials (along with the guidance produced by NCSC-FI) can be shared by our ministry, other state offices and other organisations we work closely with.

We believe that we reached at least active elderly people who use internet and IoT devices.

We asked The Finnish Association for the Welfare of Older People to be a write an article on our website. We hope that it gave us new audiences and raised cyber awareness among that target group at least a little.

https://www.kyberturvallisuuskeskus.fi/en/news/guest-writer-updates-under-control-seniorsurf-helps-elderly-go-digital

We also published a press release about the ECSM 2021 campaign. Our news monitoring picked up a few articles about cybersecurity month and top cyber tips (with links to NCSC-FI's website).

Conclusion

We should keep ECSM going. Many people already know that October is Cybersecurity Month and you should #ThinkB4UClick. Long term and persistent campaigning must and will bring results.

It could be better if we focused on fewer materials. (After the pandemic) TV, newspapers and ads for example in public transport could bring new audiences to ECSM. We also need a good budget and decent resources.

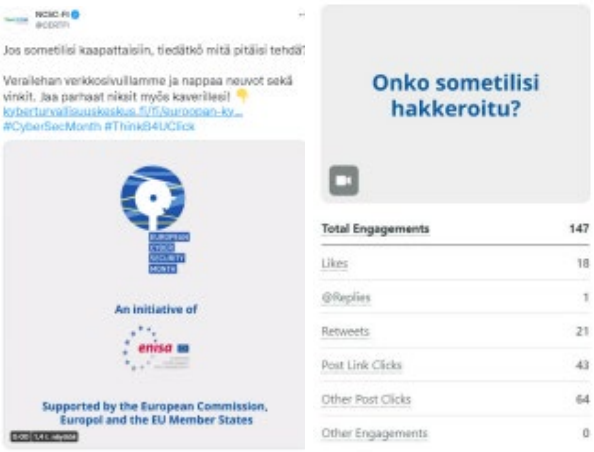
Campaign Visuals

Here are a couple of clips from our most liked ECSM tweets and our campaign website.

This tweet with a short video started the CFA weeks.

https://twitter.com/CERTFI/status/1450028690407055362

This is the Finnish version of the theme “Has your social media account been hacked?”
https://twitter.com/CERTFI/status/1450730014475960321



And finally here's a clip from our ECSM campaign website

https://www.kyberturvallisuuskeskus.fi/en/european-cyber-security-month

Greece

Exposition
Now, more than ever, education on digital security is key for citizens to identify risks and react effectively to cyber threats. In Greece the Greek Safer Internet Centre has undertaken the role of the country coordinator of the European Cybersecurity Month of ENISA. The Centre in its current form was launched in July 2016 under the auspices of the FORTH, in particular the Institute of Computer Science. It provides information, assistance and support to young and adult internet users by developing three distinct pillars:

- The SaferInternet4Kids.gr portal, where one can get informed and learn more about the safe use of the Internet, social networks and download resources.·
- The Help-line, where qualified psychologists provide support and advice on issues related to online social-emotional difficulties,
- The Hotline SafeLine, which receives reports about illegal use of the Internet and works with both the Greek Police and EUROPOL through European Agency INHOPE.

Problem
In today's digital world it is important to be digitally literate and to always think one-step ahead when utilising the net. What's more, the COVID-19 pandemic has underlined the importance of cybersecurity.

Resolution
Awareness raising through different campaigns. Specifically ECSM is the European Union's annual awareness raising campaign dedicated to promoting cybersecurity among citizens and organisations, providing up-to-date security information through education and sharing of best practises.

Result
The Greek Safer Internet Centre has been very active in the ECSM Campaign 2021. The results of this year's campaign are the following:

- The Greek SIC, together with the Hellenic Cybersecurity Authority, produced two videos. One about Passwords https://saferinternet4kids.gr/video/εσείς-ξέρετε-από-passwords/ and one about Scams https://saferinternet4kids.gr/video/smishing/
- It organised two webinars about cybersecurity with 350 high school students in each session.
- It made a successful online campaign with the materials that ENISA produced for the themes "Being Cyber Secure from Home" and "First Aid".
- The Greek SIC recruited four ECSM Ambassadors. The Greek School Network https://www.sch.gr/, NGO Together for Children https://mazigiatopaidi.gr/, many High Schools from Greece (1st High School of Zografou, etc) and the National Cybersecurity Authority.
- It organised a Facebook Live event on the 22 of October, with main guest the Secretary General of Telecommunications & Posts at Government of the Hellenic Republic - Ministry of Digital Governance, Dr. Athanasios Staveris, where he gave a talk about cybersecurity and Awareness raising in Greece. 1,164 people were reached. https://www.facebook.com/events/400784481518410

Campaign Visuals

Figure 1 Live Event Poster

Figure 2 Video about Passwords

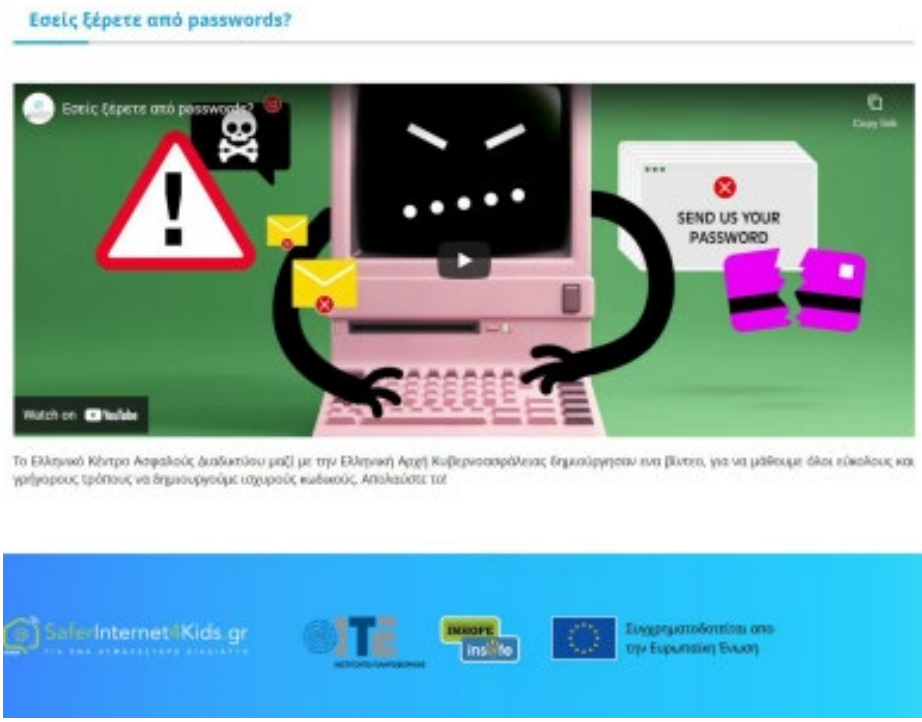


Figure 3 video about Smishing

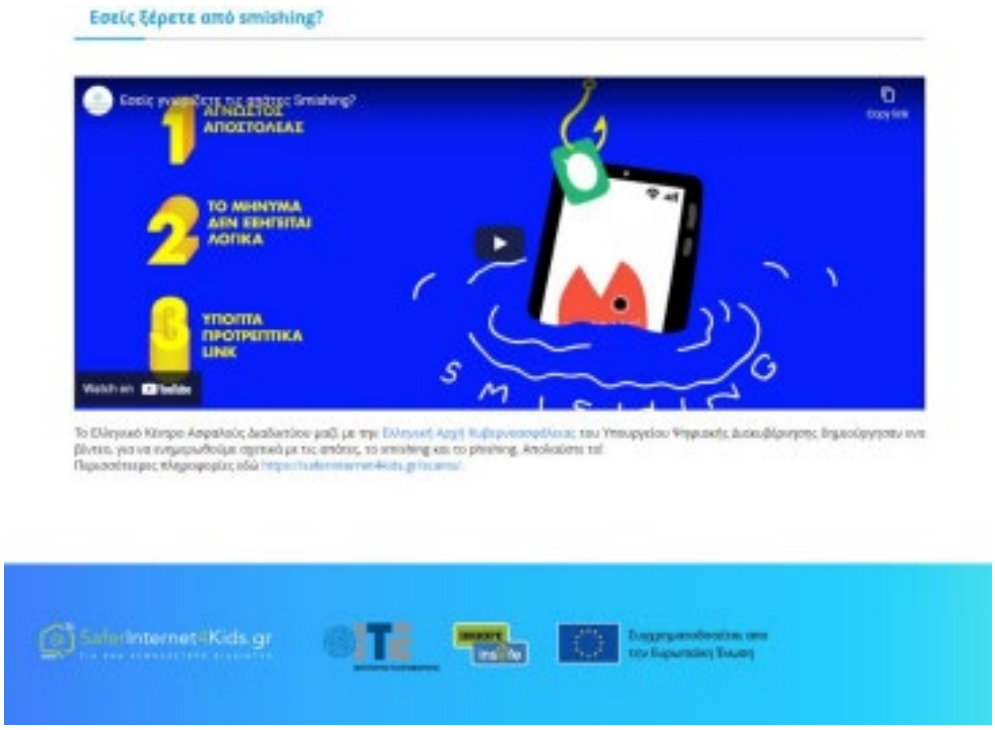


Figure 4 Presentation slide from webinars

Hungary

Exposition

Year by year in Hungary more and more organisations join the ECSM campaign. The common effort of these organisations, using continuous and clear communication tools, raises awareness of citizens. Due to the pandemic, the 2020 events were mainly organised online or remotely but this year, thanks to the lifting of the most severe restrictions, hybrid events did take place.

Problem

The main problem was the uncertainty caused by the pandemic. Thanks to this situation most of the organisations waited a lot before advertising their events, conferences, workshops, etc. Due to this lag the target audience was not fully reached.

Resolution

The National Cyber Security Centre (national ECSM coordinator) put emphasis on organising those events which have been working well for years now, without putting new initiatives in the background. It was essential to build on well-functioning initiatives to have something sure in this uncertain pandemic situation.

It should be underlined that the NCSC prepared and held events focusing on younger audiences (e.g.: The IT Security Short Movie of the Year, Hungarian Cyber Security Challenge) in order to reach a broader audience (parents, friends, teachers, etc.) through the kids.

Result

Thanks to the efforts made by the NCSC better events were organized with more professional focus, and we could tell that it was not just the 'hardcore professionals' gathered together but also new faces interested in cybersecurity.

Conclusion

This year, we can see more clearly now (and of course it is clearer for a broader audience) that cybersecurity is not just our common interest but our common responsibility.

Campaign Visuals

ECSM campaign poster

Italy

Exposition

We focused our work on the ECSM campaign and its purposes to make colleagues and partners aware of cyber threats and of cyber attacks. The pandemic, which we are all facing, has increased the use of the internet as well as different services provided online. Everyone must be protected and helped by reaching out first to national services and must protect her/himself from cyber attacks. Our objective was to use the ECSM campaign materials in the best possible way in order to raise the awareness of all stakeholders.

Problem

We immediately appreciated the materials proposed.
Therefore, our first question was how to use ECSM campaign materials to achieve our objectives and how and when to share the materials within our organisation

Resolution

We were informed the materials would have been distributed among countries members by respecting a schedule. Therefore, we decided to share our objectives with our colleagues in the Communication Dept. By working together, we realised that the materials were very impactful and had a high potential to make our stakeholders aware of the purposes of the ECSM campaign.

Result
The materials were regularly shared on the website of our Directorate-General for Communications Technologies and Information Security. Our stakeholders appreciated the video uploaded on our YouTube channel. Several colleagues were impressed by the high potential of the materials shared and they used the material with their families, friends and personal contacts.

Conclusion

We were able to achieve our objectives. By working together we raised awareness both for ourselves and for several stakeholders, that everyone needs to be cyber secure from home and everyone can count on cyber first aid.

Luxembourg

Exposition

Background
Raising Cybersecurity awareness has been on the agenda in Luxembourg for over 20 years, starting at the ministry of the Economy when in 2000, the amateur virus 'I love you' (a malicious file attached to an email with 'I love you' in the subject) hit the world. Realising the new and huge need of teaching cyber risk awareness to internet users, a couple of IT experts of the information security service within the ministry of the Economy started off, preparing sessions for civil servants as well as company employees. Thanks to the cooperation with the Luxembourg Ministry of Education, Children and Youth these classes also became accessible to the general public and primary schools. The latter grew into a dedicated initiative coordinated by the National Youth Service, known as BEE SECURE. The former grew into a grouping of economic interests known under SECURITYMADEIN.LU, representing today the national Cybersecurity Agency for the Luxembourg Economy and Municipalities. As part of the Agency's continuous developments, the newly created CYBERSECURITY LUXEMBOURG, represents the national cybersecurity portal, gathering all public and private cybersecurity actors.

When, in 2012, the Commission and ENISA decided to dedicate the month of October to awareness raising, it seemed natural to combine, where possible, that information into already existing awareness raising efforts undertaken by BEE SECURE for the general public and by SECURITYMADEIN.LU for the more business-related audience. It was also a straightforward solution to participate locally in the ECSM with little budget or human resources.

Problem
With the new mandate for ENISA in 2019/20, the mission and scope of the ECSM have grown to a bigger level, and the campaign management changed accordingly: the target group 'citizen/consumer' has come more into the focus; a promotional kit is available, clips and infographics have improved; a social media strategy has been developed, the quiz renewed, national ECSM ambassadors are being identified; the campaign evaluation scheme is being re-framed.

Luxembourg proves a strong commitment to 'cybersecurity awareness' year- long thanks to the national Cybersecurity Agency and the month of October is a visible moment of these efforts for the local cybersecurity stakeholders who contribute to the 'Luxembourg Cybersecurity Week'.

Nevertheless, with the professionalisation of the ECSM at European level, some adjustments can be undertaken locally to reflect the growing importance of the campaign and its material.

Resolution
2021 is a transition year; changes at local level may take another couple of years. For the time being, local ECSM campaign issues were addressed as follows:

- Visibility of the local ECSM opening and closing, through local press releases on the ministry's news home page.
- ECSM mentioned in ministerial speeches during October
- Dedicated place for the ECSM on the 'Luxembourg Cybersecurity Week' as part of the CYBERSECURITY LUXEMBOURG platform. The platform is work in progress; an 'EU' section is being prepared.
- With regards to languages: RESTENA Foundation partnered with the 'Géant' association, the collaboration of European national research and education networks, and within that framework, some information in Luxembourgish was made available.

Result
The 'Luxembourg Cybersecurity Week' (CSWL) organised by the Cybersecurity Luxembourg ecosystem took place successfully between the 18th and 28th of October, featuring more than twenty events, mostly online, gathering a total of over 1000 participants. 6 rewards were distributed, celebrating 7 individuals or organisations for their contribution to cybersecurity during the closing Gala.

CSWL is an event well-known by the public, and discussions taking place here often lead to partnerships and common projects. This year a delegation from France and Germany were invited to discuss common issues and exchange best practises in cybersecurity.
Synergies have been initiated and will be further developed between national and international players/partners.

Furthermore, the Gala award winners act as ambassadors all year long for how to do 'IT in the right way', which is inspiring for those working in the field, and those considering a career path in cyber.

The European Consumer Centre Luxembourg (CECL) was also part of the October activities, with an inspiring week on 'aspects of European consumer law'.

Addressing students, teachers and the public at large, BEE SECURE launched its annual campaign ' Super User How connected are you'. It is too early to talk about results, but here also it is a well-established initiative, answering the information needs of the general public.

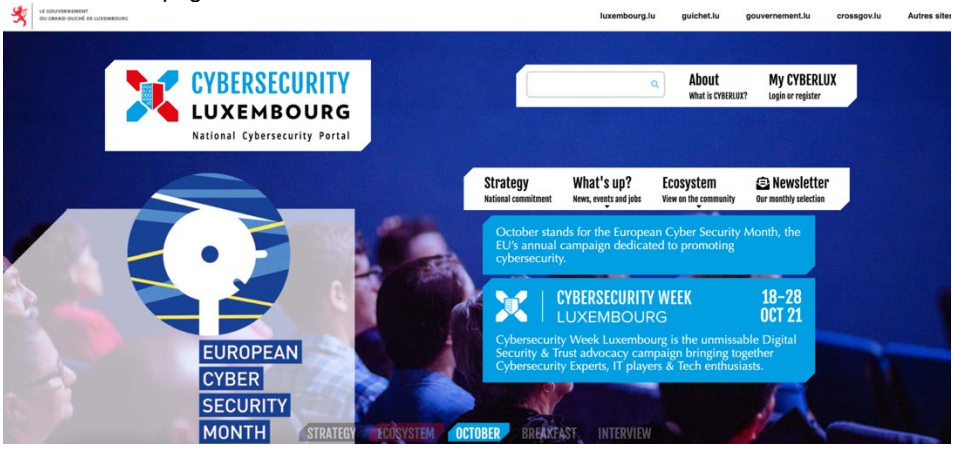
Cyberday.lu was a successful event bringing together university students, experts and researchers. This event contributed to the value of sharing problems and lessons learnt from cyber risks. It also promotes the value of undertaking studies in cybersecurity.

Conclusion
While at national level local initiatives in the field of awareness raising were running before ECSM was created, the fact that the ECSM now has a fully-fledged campaign is certainly an advantage to better reach the user with a coordinated European message. Cybersecurity is a shared responsibility and at national level we will continue to support the ECSM.

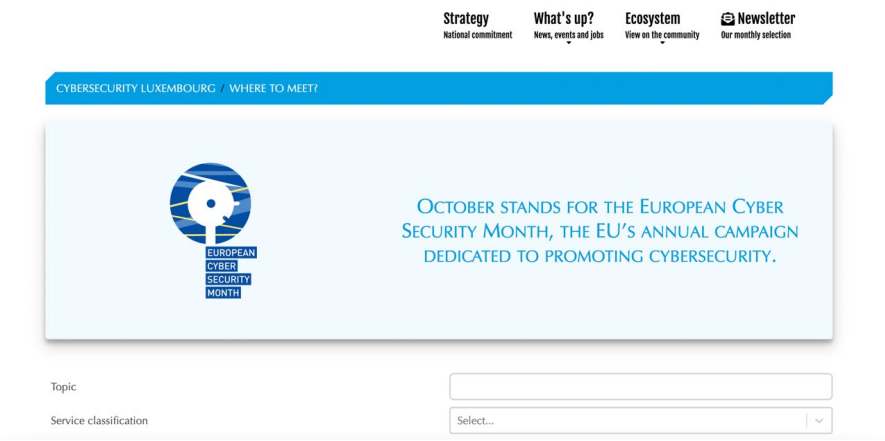
Some campaign visuals:

CYBERSECURITY Luxembourg Newsletter visual:

Banners used on cybersecurity.lu website:
Dedicated slider on the homepage with links to ECSM website & cswl.lu:



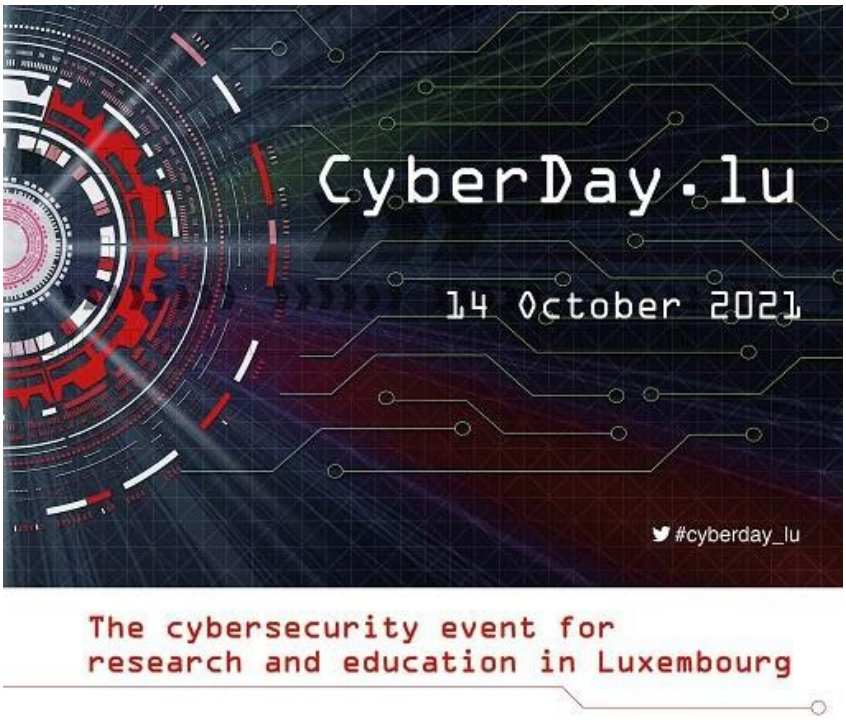
ECSM dedicated banner on the events page:



Cybersecurity week Luxembourg visual:

Gala Awards Night visual:

Cyberday.lu by RESTENA Foundation:



Malta

Exposition

As our lifestyle constantly evolves, the necessity to embrace technology has increased in due course. This has brought up new challenges and increased the probability of humans being more susceptible to cyber criminals and their tactics. One of the main factors was the COVID-19 pandemic which rapidly endorsed the need for uptake. Accordingly, we have seen multiple types of attacks, namely supply chain attacks, ransomware, phishing, spoofing, and credential theft. For this reason, Cyber Security Malta engaged in a series of awareness campaigns to educate the general public how to detect and react to cyber-attacks.

Problem

Attacks are constantly evolving and Malta is a target too.
There is a shortage of platforms where communities, mainly, techies and executives, can discuss cybersecurity matters, seek advice or knowledge of how certain attacks can be prevented or mitigated.
Besides the known attacks that have impacted Europe, around August multiple entities and non-governmental organisations were the main targets of spoofing attacks. Locally, media houses and news agencies had their websites impersonated with the aim of spreading fake, misleading news about current affairs in Malta.

Resolution

The national cybersecurity conference aimed to address different dilemmas and cybersecurity concerns both from a technical and an executive perspective. For this reason, national and world-renowned speakers approached these concerns with their years of experience, knowledge, and research in the field by participating in panel discussions, delivering presentations and demonstrations. The conference can be accessed all throughout the year by visiting and registering: cyber ROOT 21 Registration

In addition, Cyber Security Malta intensified its awareness and education campaign to the general public by participating in a number of television programmes, radio shows, news features, and newspaper articles, apart from social media. For the month of October, Cyber Security Malta tackled the fake news subject by utilising a renowned Maltese personality and a Maltese police inspector within the Cyber Crime Unit, who are coincidentally, twin brothers.

Result

This year's cybersecurity conference, although presented in the form of a webinar, saw an increase in the number of attendees and participation throughout the conference.

Exposure has been given to Cyber Security Malta on various platforms, namely, TV, radio, online portals, and traditional newspapers as well as on social media. Given the reach and query for assistance received, the awareness of the general public was raised and there is the desire for more information.

Conclusion

Every campaign is unique. Campaigns should focus on the demand that is needed in each member state, and engagement should be throughout the year not just during the month of October for cybersecurity month.

Campaign Visuals

Mr.Robert Muscat alongside Mr.Timothy Zammit, the Cyber Crime Unit police inspector, (left to right) featuring on Realta' a Maltese TV program on the national TV channel, TVM.

Mr. Roderick Lia (right), Cyber Threat Intelligence Senior Project Leader, discussing various topics related to the cybersecurity on Radju Malta.

Mr. Martin Camilleri, Cyber Threat Intelligence Manager, presenting at this year's Freshers Week.

Fake News Awareness video showcased by Mr. Timothy Zammit, Police Inspector with Malta Cyber Crime Unit, and Mr. Frank Zammit, a Maltese personality (left to right).

ICT

mita

Cyber spoofing tactics, techniques and procedures

RODERICK LIA

The term 'spoofing' or 'spoofed' has recently been mentioned and used quite often within the local domain.

Yet throughout the years, different Maltese strata were targeted, amongst whom, high profiles like Prime Ministers, Leaders, Presidents as well as entities and non-governmental organizations. It is therefore of utmost importance to understand what spoofing is, the motivation that impostures might have, the different forms of spoofing and how one can notice digitally spoofed content.

A spoofing attack within the cyber security domain is when an impostor pretends to be someone or something else to gain a person's trust. Spoofing typically consists of two main elements. There is the spoof itself that could be a faked website or email, and the social engineering aspect that leads the victim to take an action against a specific request being made by the impostor. An example that everyone might relate to is the email that appears to come from a trusted and known senior employee requesting a payment or settlement of outstanding bills. Impostors utilize techniques like these to manipulate and encourage victims to carry out the desired action without raising alarm or suspicion. Such activity sometimes adopts different levels of technical complexity. But not just that. It also uses a set of social engineering techniques and psychological manipulation that could potentially instil a sense of fear, reputational damage as well as destabilization.

Spoofing attacks can be noticeable or unnoticeable to victims. Irrespective of this, a spoofing attack can lead to serious implications. Some of the known consequences are the stealing of digital identities, known as credentials, personal or company's information, involvement in malware sharing and spreading, access to unauthorized systems as well as to becoming victims to ransomware attacks.

Different types of spoofing attacks exist. The most common ones are the emails mentioned above, websites, phone calls and text messages.

The Email spoofing attack can occur in two different formats. The first format is when a malicious actor forges the email content, known as the email headers and changes the display name of the email address. The second type involves the utilisation of the same victim email address and send email through unauthorised services. Given that most users take this at face value, being a victim to such attack is quite common. Some common reasons why spoofed emails are sent vary from, these being from requests for money transfer, to seeking permission to access a particular system. To a certain extent, spoofed emails might even contain attachments that once opened trigger the installation of malware such as Viruses and Trojans that could potentially spread across all the entire network.

The Website spoofing attack, that is also known as URL spoofing, occurs when a scammer builds a fraudulent website that resembles an authentic and already established site or brand. Spoofed websites usually portray the logos, branding and images stolen from the authentic site. In certain cases, an identical login page is also presented. Even though the spoofed URL appears to be correct at first glance, in reality an extra or a truncated character, such as a number or symbol would point to a different site; this method is known as Typosquatting. We have even seen instances where website spoofing URLs have been placed in conjunction with an email spoofing. Therefore, the scammer is using the email medium that will lead the victims to access fake websites. Some common reasons why spoofed websites are part of the hacker's favourite lists, is that they enable hackers to steal credentials as well as to drop malware and infect devices and computers.

The Phone call spoofing attack, also known as Caller ID spoofing, occurs when scammers intentionally forge the caller ID details to mask their identity. We all know that a local number is more likely to be picked up than a number which is not recognize. In such type of spoofing a VoIP (Voice over Internet Protocol) is used. This will allow scammers to create a phone number and caller ID of their choice. The main scope of such an attack is to obtain sensitive information including credentials to systems once the phone call is answered.

The Text message spoofing attack, also known as SMS spoofing is when the sender of a text message crafts a message that misleads recipients with fake displayed sender information and thus pretends to be a legitimate business or a government department. The reason behind such SMS is to deliver links that could offer malware download, spread fake news as well as obtain system credentials.

Although spoofing attacks are on the increase and becoming more complex, online safety protocols may help to minimize one's exposure to a spoofing attack. The following Do's and Don'ts can help in this regard:

Don'ts

- Do not click on links or open attachments from unfamiliar sources.
- Do not answer emails or calls from unrecognized senders.
- Do not give out personal information online.

Do's

- Where possible, set up two-factor authentication.
- Use strong passwords.
- Review your online privacy settings.
- Keep your network and software up to date.

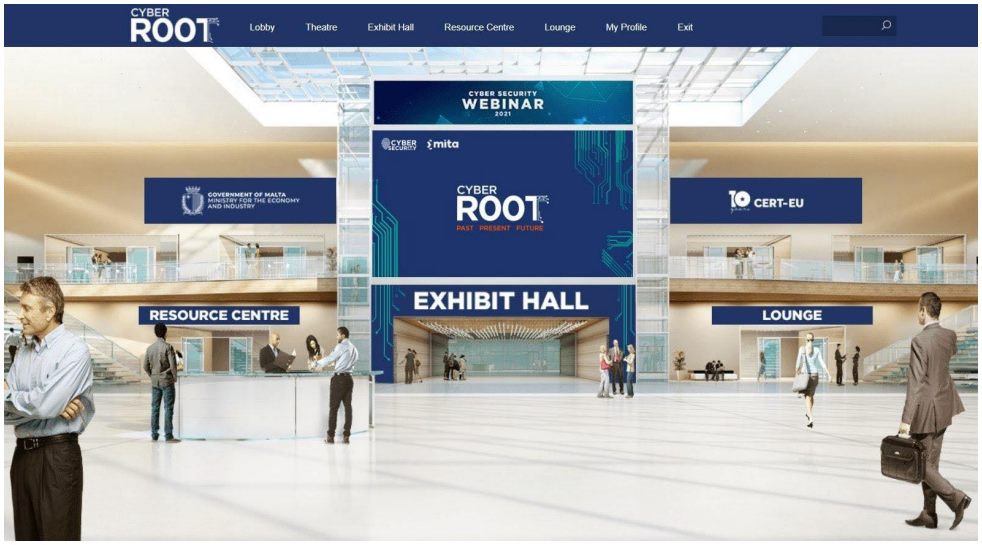
As a final remark we advise that websites, emails, or messages with poor spelling or grammar and any other features that look incorrect, such as logos, imagery, colour scheme and branding, or missing content, could be a sign of a spoofing attack, and therefore should be ignored or verified, and when necessary reported to the respective authorities.

Roderick Lia
Senior Project Leader,
Cyber Threat Intelligence, MITA

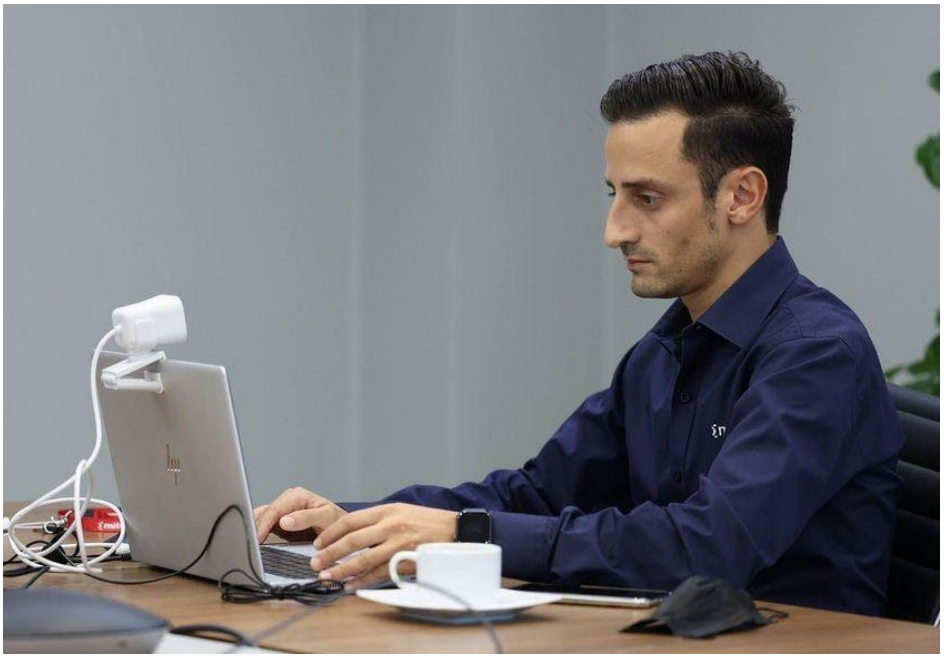
The Malta Independent ICT Feature: MITA Communications and PR Team – All ICT Features are available on www.mita.gov.mt/ictfeature

Article written by Mr. Roderick Lia https://bit.ly/3uSelmc

Mr. Ryan Emanuel Bugeja, Senior Solutions Architect, featured on Carter Jirrapporta – Dark Web on the national TV Channel, TVM.



Cybersecurity Webinar Conference 2021 Platform



Mr. Reuben Gauci, Security Operations Project Manager, highlighting the experiences and challenges encountered in dealing with cyber events, and what can be done to prevent future cyberattacks at the Conference.

Mr. Antoine Debono and Mr. Robert Muscat (left to right), Information Security Specialists and Session Facilitators at the Conference discussing the supply chain attacks.

Portugal

Exposition

Portugal still has insufficient results in terms of attitudes and behaviours towards cybersecurity, especially considering the best practises of cyber-hygiene. This conclusion has been reached in several reports produced by the Cybersecurity Observatory of the Portuguese National Cybersecurity Centre. As a result of this, a social network campaign was developed using traditional and popular sayings, or proverbs, that are very common in the way people talk with each other in everyday life. Each one of these proverbs was articulated with a specific cyber-hygiene practice. For instance, one popular saying in Portugal is “In the land of the blind, the one-eyed man is king”. In the campaign, the following advice was added to this proverb: “read your emails carefully, do not click on unknown attachments or links”. By doing so, it was possible to, in a simple and direct manner, make a relation between what people know (the proverb) and what they must learn (cyber-hygiene practises). That was very efficient in terms of reactions. Graphically the content had a background of traditional Portuguese tiles, stressing the popular and traditional elements of the message, and communicating with all generations. The name of the campaign was “In the cybersecurity month, popular wisdom might help”.

Problem

The insufficient results in terms of attitudes and behaviours towards cybersecurity in Portugal, especially considering the data produced by the Cybersecurity Observatory of the Portuguese National Cybersecurity Centre: https://www.cncs.gov.pt/pt/observatorio/

Resolution

The campaign was launched in several social networks, and distributed by different stakeholders, who helped CNCS in the dissemination of this content in their own social networks. Some of these proverbs were also inscribed on tiles and offered in CNCS’ annual conference C-Days. In terms of communication, the results were very good: the reactions, the interactions, and the audience numbers.

Result

Although there were very good results in terms of communication, we still must make a deeper analysis of the impact on citizen’s behaviour, especially if we want to establish a correlation between specific campaigns and behavioural change. Next year we plan to develop research about the impact of the awareness and training strategies and content on society. This work will be developed under the scope of the CNCS’s Cybersecurity Observatory.

Conclusion

It is important to create clear messages that highlight what to do, instead of just promoting fear in people. It is also very important to relate the message to prior knowledge people have about other subjects, to help in the interpretation and assimilation of the message. In the future, we must make a deeper analysis of the impact on behaviour, establishing a correlation between specific campaigns and behavioural change.

Campaign Visuals

"To pay and die are the last things to do".
DO NOT CONTRIBUTE TO THE COMPUTER CRIME. DO NOT PAY RANSOMS.

"Laziness is the mother of all vices".
TURN ON THE MULTIPLE FACTOR OF AUTHENTICATION WHENEVER IS POSSIBLE.

"Business is business".
IF ON SOCIAL NETWORKS SOMEONE ASKS YOU FOR MONEY, BE AWARE.

"Water dropping day by day wears the hardest rock away.".
AN ATTACKER WON'T GIVE UP AT FIRST, USE STRONG PASSWORDS (10 characters, uppercase, lowercase, numbers, and special characters).

"In the land of the blind, the one-eyed man is king".
READ YOUR EMAILS CAREFULLY, DO NOT CLICK ON UNKNOWN ATTACHMENTS OR LINKS.

"Forewarned is forearmed".
SAVE THE RECORDS OF THE YOUR TRANSACTIONS AND ONLINE SHOPPING.

"An elephant memory..."
IS TO HAVE A BACKUP DISCONNECTED FROM THE NETWORK.

"Don't give the gold to the bad guy."
AVOID SHARING PERSONAL DATA ONLINE.

"Not all that glitters is gold".
CHECK IF THE SHOPPING WEBSITES YOU VISIT ARE TRUSTWORTHY.

"Better be safe than sorry".
CHANGE YOUR PASSWORDS OFTEN.

"When the alms are too good, the poor one distrusts".
DON'T BELIEVE IN OFFERS ONLINE THAT ARE TOO GOOD.

"Who tells a tale adds a tail".
CHECK, DO NOT SHARE FAKE NEWS.

"Better to ask the way than go astray."
CONTACT THE AUTHORITIES IF YOU ARE A VICTIM OF FRAUD

"Who sees faces does not see hearts".
CHECK THE REPUTATION OF THE SELLER BEFORE YOU BUY ONLINE.

Romania

Exposition

Online Safety campaign with Romanian Police and Romanian Banking Association
In Romania we focussed the ECSM 2021 around the two themes voted at EU level – First Aid to Cybersecurity and Working from Home, while touching on the most pressing types of attacks that target common users – scams.

For this, together with the Romanian Police and Romanian Banking Association we launched a national online safety campaign, which is actually an extension of a previous campaign for marketplace platforms' clients. We launched a website for this https://sigurantaonline.ro, where users can educate themselves on the most common scams. We also launched a quiz here, so that visitors can test their ability to detect such scams and train themselves on how to spot them. Every question from the quiz has a scam sample or a legitimate message and the user has to spot which one is which. If the answer is wrong, they will be able to spot the signs that would've raised questions otherwise, if they were paying enough attention.

This campaign was supported through mainstream media in Romania and was promoted with 3 videos that were broadcast by the most popular Romanian television stations as public awareness messages. Moreover, these clips also played in Bucharest on the screens of public transport vehicles, of private banks and some popular shopping malls.

Quiz: https://quiz.sigurantaonline.ro/
Videos: https://youtu.be/2JHBdsbR4Nw, https://www.youtube.com/watch?v=Bs6rdiwm1VY

We also published with ISACA Romania a book during ECSM 2021: Keep Your Information Safe, which is in English and can be read/downloaded/distributed from our DNSC website:
https://dnsc.ro/vezi/document/keep-your-information-system-safe-kiss

The aim of this book is not only to put together some principles, methodologies and any other relevant theoretical aspects on critical cybersecurity topics (offensive security, security incident handling, healthcare and supply chain security challenges, etc.) but also to provide an end-to-end overview of such selected topics and provide guidance on practical aspects for implementation, based on their own experience and perspective.

Moreover, the content makes for accessible reading independent of the level of seniority a specialist might have. If you are a beginner, then this is a perfect way to gain insight into the topics and an invitation to start searching for additional materials depending on your needs and curiosity. In case you are a senior in the area, then you might find the information helpful as a means to compare and validate your approach and vision but at the same time it might give you new perspectives on specific topics.

Slovenia

Exposition

In the last couple of years, we have noticed a steady increase in the number of cyber attacks targeting small and medium sized business enterprises. Financial losses that SMEs suffer as a result have also been growing and, according to our data, reached an all-time high in 2019.

Problem

SMEs are becoming a very popular target for cyber criminals as they often do not have the resources to implement sufficient cybersecurity measures. Additionally, they often do not employ IT experts, nor educate their employees on cybersecurity. As a result, their employees do not possess the knowledge or skills to recognize and protect themselves against cybersecurity threats.

Resolution

Cybersecurity has never been this important and to raise the level of awareness, we decided to launch a free online course “Safe in the office” (SI: Varni v pisarni – www.varnivpisarni.si). Since employees are usually short on time, we opted for a video format as we figured this was the best way to relay the information in a quick and concise manner. We divided the content into 4 modules, each addressing dangers pertaining to a specific job position (basics, marketing/sales, administration/finances, and IT). Each module covers topics that we split into 2-to-3-minute clips, so that viewers could watch the course at their own pace. In order to make the course more interesting, we included humoristic breaks with Jože Robežnik, who was the main character of our previous 3-video series. At the end of every module, we included a short quiz to test the viewers’ knowledge. If completed successfully, the user received a certificate that proved they had attended the course.

Result

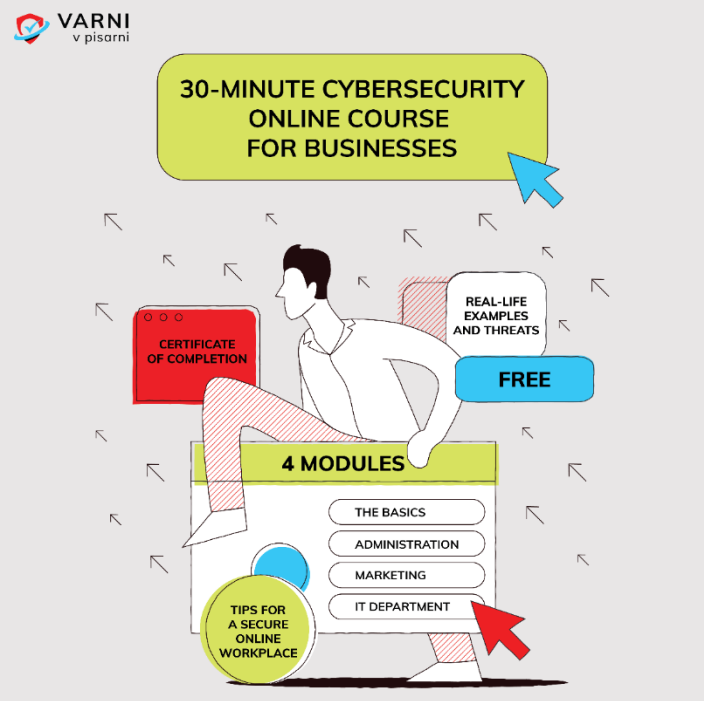
This online platform will be an on-going project and we hope that many businesses (and individuals) will decide to take the course. Certain companies, who have discovered our course, have already instructed their employees to complete one or more modules. So far one thousand users have registered and taken the course and the feedback has been very positive.

Conclusion

The majority of cyber attacks are still a result of human error, which is why we believe that the best protection or “antivirus” is knowledge. By offering this free course, we are giving each user the opportunity to educate themselves on cybersecurity and obtain the necessary knowledge and skills to stay secure in the workplace.

Campaign Visuals

Promotional flyer



Tadej Hren, cybersecurity expert at SI-CERT

Tadej Hren and Jože Robežnik

Varni v pisarni webpage

Spain

Exposition

The national cybersecurity culture is an issue of paramount importance for Spain. Our National Cybersecurity strategy identifies the need for greater input from everyone in society by encouraging a cybersecurity culture, to evolve from awareness to action, in the understanding that citizens have joint-responsibility for national cybersecurity.
Promoting cybersecurity culture should be one of the central themes being developed to make society aware of these threats and challenges. The right to secure, reliable use of cyberspace and contributing to this situation are shared responsibilities.
The aim is to establish one specific goal dedicated to culture and commitment to cybersecurity and strengthening human and technological skills. This goal is developed through a Line of Action for developing a cybersecurity culture that includes eight specific measures and is aligned with the National Security Culture Plan. This Culture Plan is a broad and ambitious project included in the National Security Law.
Public-private collaboration is essential for improving national cybersecurity culture.
Considering the above mentioned strategic and legal umbrella, European Cybersecurity Month offers us an opportunity to develop actions aligned with this. In that sense, Spain has organised a set of activities to promote awareness and culture in cybersecurity, focusing in the different targets:

- Increase awareness-raising campaigns for citizens and companies
- Boost initiatives and plans for digital literacy in cybersecurity.
- Promote the spread of cybersecurity culture as a best business practice
- Promote awareness-raising and training on cybersecurity in schools, adapted to all training levels and specialties

14 activities were uploaded and promoted through ECSM website.

The CCN carries out the following activities:

- Cyber advice https://www.ccn.cni.es/index.php/es/ciberconsejos
- STIC CCN-CERT Conference https://www.ccn-cert.cni.es/en/xiiconference
- ENS meeting. Security Trends and Policies https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/encuentro-ens
- Conference on Early Warning System (SAT)

INCIBE offers companies tools to help them make cybersecurity their differential value, as well as to give them the ability to protect themselves, become aware of the problem and, when appropriate, prevent possible incidents. These tools include the blog and security notices, the antibotnet service, which in the case of companies allows them to know if any computer equipment is being controlled remotely. Another useful tool is the self-diagnostic kit so that companies can evaluate their level of cybersecurity through some simple questions and thus be able to improve their protection against possible risks and threats. INCIBE also offers an anti-ransomware service (extortion that arises after the "hijacking" of device information by a virus), a catalogue of companies and cybersecurity solutions, and a role-play game that makes it possible to simulate five incidents, along with their solutions Among the training elements, there are online courses under the MOOC methodology, interactive sector pathways and a "serious game" on cybersecurity, called "Hackend, the game", which helps players learn the most important risks faced by professionals.
This free game won the prestigious "Best Serious Game" award in 2016 at the Serious Fun Games Festival.

Professionals in the cybersecurity sector.
INCIBE has several instruments to serve this sector that include

- Blog
- Security notices
- Antibotnet service
- Self-diagnostic kit
- Anti-ransomware service
- Catalogue of companies and cybersecurity solutions
- Role play
- Online courses
- Sectoral interactive itineraries
- “Hackend, the game”
- Professionals in the cybersecurity sector
- Security notices or notices for professionals in industrial control systems or vulnerabilities cybersecurity log or guides and studies.

Citizens:
INCIBE has the Internet Security Office (OSI) as an awareness channel focused on all those citizens who use the Internet on a regular or daily basis, without having advanced knowledge of computer science, telecommunications or cybersecurity. For that, it has several instruments, such as the blog, security advisories, true stories, the CONAN

mobile service and the previously mentioned anti-botnet service, the cybersecurity test and two "serious games" called "Cyberscouts" and "Hackers vs Cybercrook" and a telephone service to answer citizens questions and solve security problems. There is a blog, security notices, real stories, the CONAN mobile service, antibotnet service, cybersecurity test, “Cyberscouts”, “Hackers vs Cybercrook”, telephone service.

For Minors:
INCIBE has the Internet Safety Centre for Minors in Spain or Safe Internet for Children (IS4K) to promote the safe and responsible use of the Internet and new technologies among children and adolescents. With it Spain will align with the Better Internet for Kids (BIK) strategy of the European Union, which seeks to sensitise and train not only minors, but also their immediate environment: family, teachers, educators and professionals of the sector, in Safe and responsible use of the Internet and new technologies. For this, it has several instruments such as parental control tools, the preparation of teaching materials for the educational community, the kit for educators, and the knowledge test.

It also has different programs:

- Cyber Olympics aimed at secondary schools and higher education colleges nationwide,
- "Your space in cybersecurity" Stand
- Organisation of the Safe Internet Day, in Spain.
- Parental control tools
- Teaching Kit for educators
- Knowledge test
- School days
- Cybercamp aimed at families
- Cyber volunteers

IT, SCI and cybersecurity professionals: https://www.incibe-cert.es/
Cyber Professionals: https://www.incibe-cert.es/
Businesses: https://www.incibe.es/protege-tu-empresa https://www.incibe.es/protege-tu-empresa/kit-concienciacion
Citizens: https://www.osi.es https://www.osi.es/es/campanas
Minors : https://www.is4k.es/ https://www.is4k.es/campanas

In July 2020 Spain approved the National Cybersecurity Forum, a public-private initiative included in our National Cybersecurity Strategy 2019. This Forum will focus on creating synergies, particularly generating knowledge on opportunities, challenges and threats to security in cyberspace. The Forum incorporates representatives from civil society, experts, private sector, academia, associations. The 3 main axes that will be addressed are: culture, strengthening industry and R+D+I and promoting talent and education.

https://foronacionalciberseguridad.es/index.php/en/
The forum is set up for 16 different organisations (users, professionals, academia).
One of the working groups is dedicated to Cybersecurity Culture, and the first work done has 4 main objectives:

- Objective 1: to analyse existing national and international initiatives and trends aimed at promoting a culture of cybersecurity.
- Objective 2: to inform possible actions aimed at fostering national cybersecurity culture and generating a shared social awareness of the importance of cybersecurity.
- Objective 3: to draw conclusions on the current state of cybersecurity culture in Spain and assess areas for improvement
- Objective 4: to formulate proposals to improve the state of cybersecurity and generate social awareness of its importance.

As a conclusion of this work, the Forum proposes 65 measures to improve cybersecurity culture, one of them is the creation of the National Cybersecurity Observatory https://observaciber.es/ that offers to citizens statistics, reports and data for improving cybersecurity culture.
The Forum has been an important element in ECSM 2021 for spreading key messages and taking part in activities during the ECSM campaign.

The biggest event that took part in ECSM during October in Spain was the International Meeting on Information Security, which took place in Leon for 2 days.
https://www.incibe.es/en/enise/program

INCIBE also manages the 017 helpline that is the national, free and confidential service that INCIBE makes available to Internet and technology users in order to help them solve cybersecurity problems that may arise in their day-to-day life. It is aimed at citizens (Internet users in general); companies and professionals who use the Internet and new technologies in the performance of their activity and must protect their assets and their business; and minors and their environment (parents, educators and professionals who work in the field of minors or online protection linked to this public). The service is attended by a multidisciplinary team of experts, through the different contact options, who offer technical, psychosocial and legal advice, from 9 a.m. to 9 p.m., 365 days a year.

Finally, INCIBE has spread TV cybersecurity advice that has been broadcast on the main TV channels. The new campaign is 'Today is an ad, not tomorrow' (#HoyEsUnAnuncio), launched in 2020, and showing what could happen if a user was the victim of a cybersecurity incident. This time it was portrayed through various scenarios that gave continuity to the message about the importance of taking precautions in our digital life, providing new ways to prevent or solve any cyber incident.

Problem

Coordination between the many different agencies that cybersecurity competences are spread across in Spain is one of the difficulties that needs to be addressed.
During the national campaign we used the Standing Permanente Commission, set up by main cybersecurity public agencies; and the National Cybersecurity Forum which is composed of other forums of professionals, citizens, academia.
However we had to spend a lot of effort in coordination and the visibility of the success of the campaign was limited.
We used and spread the material made by ENISA, but perhaps it could be better, as in other years, to update the ECSM website in order to publish the material there which has been translated into the different languages and published according to the calendar. It was a little bit inefficient to send infographics every year to all actors.
This will help member states, since we only need to link actors with this website.
Another recursive problem is how to measure the impact of all the activities we developed during ECSM, because a lot of them are on the private sector side and this information was not public.

Resolution

As already mentioned, we have to put in extra coordination efforts because usually there are limited resources for the campaign.

Result

We are dedicating a lot of effort in order to improve the cybersecurity culture in all the layers and both, public and private fields.
Training courses, awareness campaigns, dedicated portals. The idea is to identify gaps and cover them with new campaigns depending on the state of the art of the cyber world, new threats, level of maturity and so on.

Conclusion

ECSM has grown up since it started. However, there are limited resources to modify national campaigns that are already in place, although the topics used are similar.
Spain has a lot of material, websites, help lines and specific campaigns for the different sectors of the public. We consider that, of course, there is an improvement opportunity, but looking to improving culture in a 360º is a correct approach for this.

Campaign Visuals

Videos

- The new campaign is 'Today is an ad, not tomorrow' (#HoyEsUnAnuncio), launched in 2020, and showing what could happen if a user was the victim of a cybersecurity incident.
  Hoy es un anuncio, mañana no | INCIBE
- Citizens https://www.youtube.com/watch?v=_K_DqXb-6vY&feature=youtu.be
- Businesses https://www.youtube.com/watch?v=edBKitPaOxQ&feature=youtu.be
- Minors https://www.youtube.com/watch?v=gsr5xZ4Ry9M

Protect your Business website https://www.incibe.es/protege-tu-empresa

- Awareness kit https://www.incibe.es/protege-tu-empresa/kit-concienciacion
- Cyber Explorer (that helps companies with cybersecurity issues)
  https://www.incibe.es/exploradorincibe

Ransomware

Phishing

Deepfake

Minors

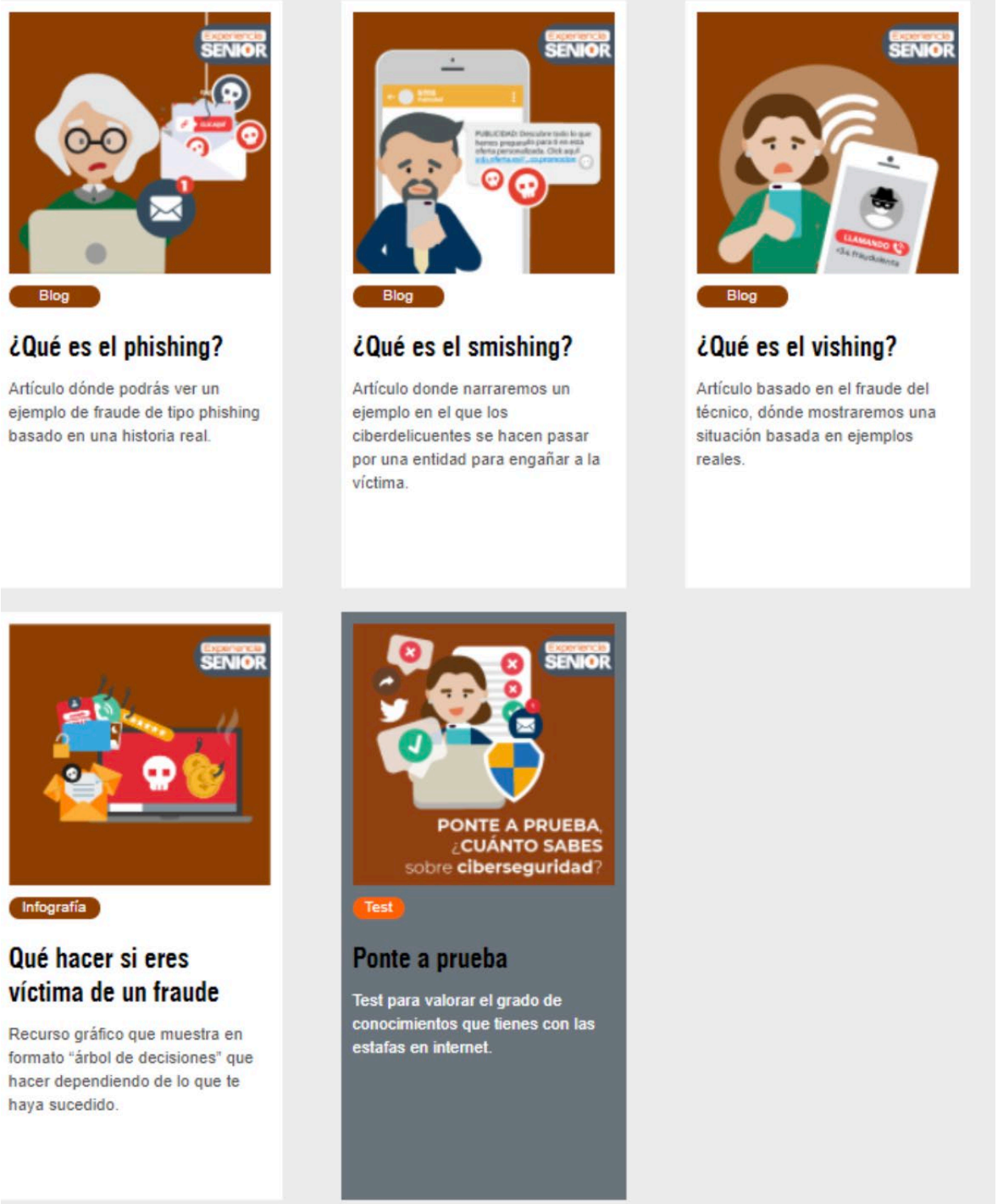
https://www.is4k.es/necesitas-saber

Other campaigns https://www.is4k.es/campanas

For senior people

Video https://youtu.be/x3NTrL0lagk

https://www.osi.es/es/experiencia-senior



Other campaigns https://www.osi.es/es/campanas

Video https://youtu.be/Djw0MNmdB7Y

Experiencia senior

Aprende desde cero las bases de la ciberseguridad de una forma sencilla y paso a paso.

Cuida tu privacidad

Controla y administra tu seguridad y privacidad de tus cuentas de la mano de Google.

Quédate en casa pero ciberseguro

Consejos para afrontar la situación de confinamiento por el Covid-19, con ciberseguridad.

Los ciberdelincuentes, ¿quiénes son?

Qué es un ciberdelincuente, sus motivaciones y en qué se diferencia de un hacker.

IoT, los riesgos de un mundo hiperconectado

Todo lo que debes saber sobre la Internet de las cosas, la domótica, los dispositivos conectados a la red...

¡Contraseñas seguras!

Comprende por qué son tan importantes las contraseñas y aprende a gestionarlas de manera segura.

Redes sociales, ¿cuánto saben de ti?

Conoce la importancia de saber qué publicar o cómo reaccionar ante los distintos tipos de publicaciones.

Dispositivos móviles

Aprende a configurar tu dispositivo para protegerte de los riesgos de seguridad y privacidad a los que estás expuesto.

Dispositivos personales y trabajo, ¿qué debes saber?

Utiliza equipos personales para trabajar teniendo bajo control los principales aspectos de seguridad.

Compras seguras online

Identifica todos los detalles que debes revisar en una web para disfrutar de tus compras

Alquileres vacacionales

Sigue las pautas que te detallamos para que no caigas en engaños fraudulentos que

¿Es seguro dónde guardas y cómo envías la información?

Public sector

https://angeles.ccn-cert.cni.es/index.php/es/

Cyber advice

https://angeles.ccn-cert.cni.es/index.php/es/ciberconsejos

Training

https://angeles.ccn-cert.cni.es/index.php/es/menu-formacion-es/itinerarios-de-formacion

ATENEA, the new CCN-CERT platform where you can demonstrate your knowledge and skills in the face of different security challenges. Here you will find challenges of varying difficulty and on very diverse themes: Cryptography and Steganography; Exploiting, Forensic, Traffic Analysis, Reversing, etc.

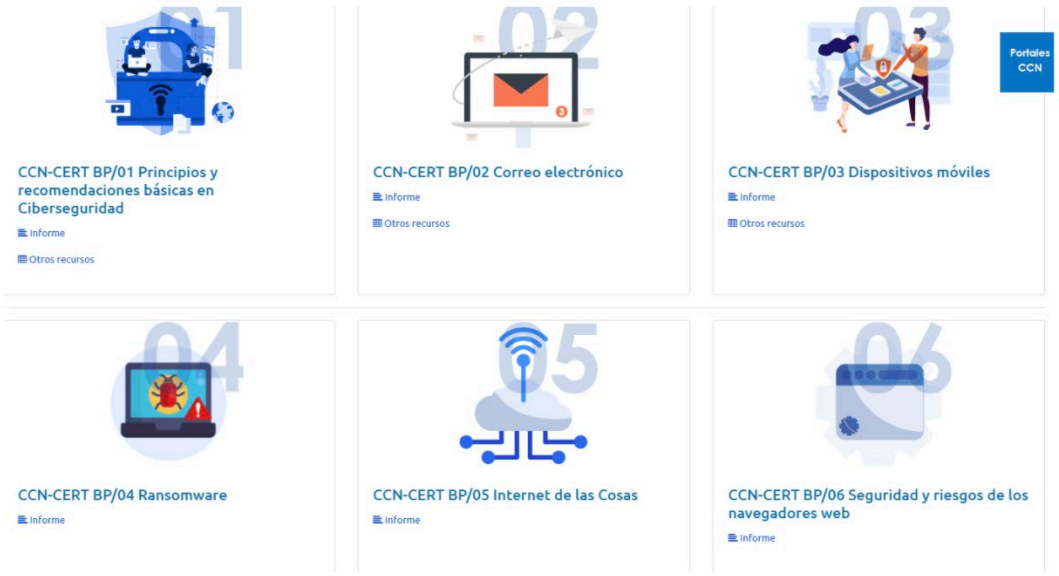
https://angeles.ccn-cert.cni.es/index.php/es/talento-es/atenea-menu-es

ATENEA School is a basic platform for computer security challenges composed of different challenges to promote the learning of users less knowledgeable in the field of security

https://angeles.ccn-cert.cni.es/index.php/es/talento-es/atenea-escuela

Good Practises

https://angeles.ccn-cert.cni.es/index.php/es/informes/buenas-practicas



Sweden

Exposition

The main objective of the campaign was to help individuals and small businesses (0-10 employees) 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 malice attacks like phishing and ransomware, eID, back-up and passwords.

Problem

The digital society needs increased awareness of new threats and vulnerabilities. The challenge is to prompt behaviour change at the individual level, which is especially challenging because our brains are built to save energy and seek reward more than it takes care to click on links. The challenge however is that the new safer behaviours that are necessary are working against what the human brain instinctively wants. It is therefore important to work long-term.

Resolution

We (MSB and the police) have for 4 years worked and deepened the cooperation between 21 organisations (banks, companies, associations, authorities, etc.). The collaboration is stronger and used more widely than the campaign and is also valuable to their own organisations. Several partners create internal project groups, which in itself contributes to an increased understanding of cybersecurity. Cybersecurity is not an individual's responsibility but a community.

We feel that each partner is best placed to reach their target group most effectively because they are a credible sender that the target group trusts and listens to. MSB and the police have overall responsibility for the campaign "Think safe" and produce about four messages each year. In addition, we have simple checklists available on msb.se. We support partners and offer freedom to work both internally (employees) and externally (customers, members, citizens), and create appropriate messages and communications materials which are most appropriate to their target group. This strategy has worked very well this year and has contributed to great success.

Result

This year, the collaboration has yielded an outstanding result. Last year we reached about 1.5 million whereas this year we reached 12.6 million!
We feel that the issue of cybersecurity has received a real increase in focus. The reason for this may be partly that Coop (food company) was hit hard in an incident in July and could not charge customers for several days, which raised awareness nationally and internationally that everyone in society can be affected - both individuals and companies.

The number of visitors to https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/informationssakerhetsmanaden/ has increased compared to before, but gives little effect overall, but still important. Partners can find useful information there. For the third year, we conducted an IT security survey for the general public, which shows that behavioural changes in the population occur very slowly. However, the survey gives us proof that the campaign is important.

The collaboration between 23 organisations has provided a base to work from, where we gather inspiration together, as well as commitment and knowledge. This year, we have also made better use of each other's expertise and collaboration, for example in webinars and lectures. In total, over 60 webinars have been conducted, with over 30,000 visitors. Several of the webinars can be seen afterwards on the web. Several were arranged by companies' organisations, such as Swedish Trade.

A webinar organised by the Internet Foundation had 4,000 visitors, which has been viewed about 6,000 times in retrospect, mainly by the older generation. Crucial to that success was the support of good partners who shared the invitation further. We will continue to work on this approach next year!
The police arranged a very successful "Think Safe" communications which gave 55,000 interactions and which was later shown on Story more than 500,000 times!

Several organisations had webinars or various internal training sessions for their employees, for example, with a focus on "working remotely", secure eID, passwords etc.

Finally, and still significantly, more people than in previous years have used newsletters, articles, emails to communicate various messages.

In addition to our partners, most of Sweden's regions, many municipalities and additional authorities were active during October, with their own material or with the Think Safe material.

Conclusion

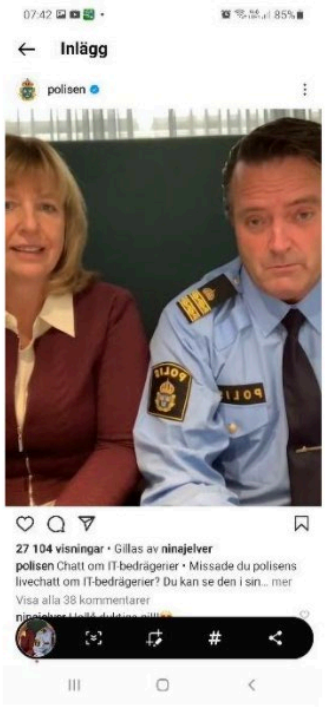
The foundation and long-term perspective are most effective when two authorities cooperate, MSB and the Police Authority.

The next step is to develop collaborations with several partners who can reach citizens and employees. Create commitment, common interest, learning and "ownership" to contribute to increased awareness and safer behaviour among citizens and employees. Give freedom and encourage to embrace cyber secure behaviour. However, we will continuously need to refresh and re-evaluate, and develop campaigns so that we can reach target groups more effectively.

Campaign Visuals

MSB's "Roger film", re-launch of campaign film from 2018

The police and several other organisations have produced various short films and a chat.



We arranged over 60 physical meetings and webinars, external and internal. They are often online and can be viewed afterwards. Here is Svensk Handels webinarium.

TP-AL-22-001-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. More information about ENISA and its work can be found here:
www.enisa.europa.eu

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-573-9
doi: 10.2824/647127