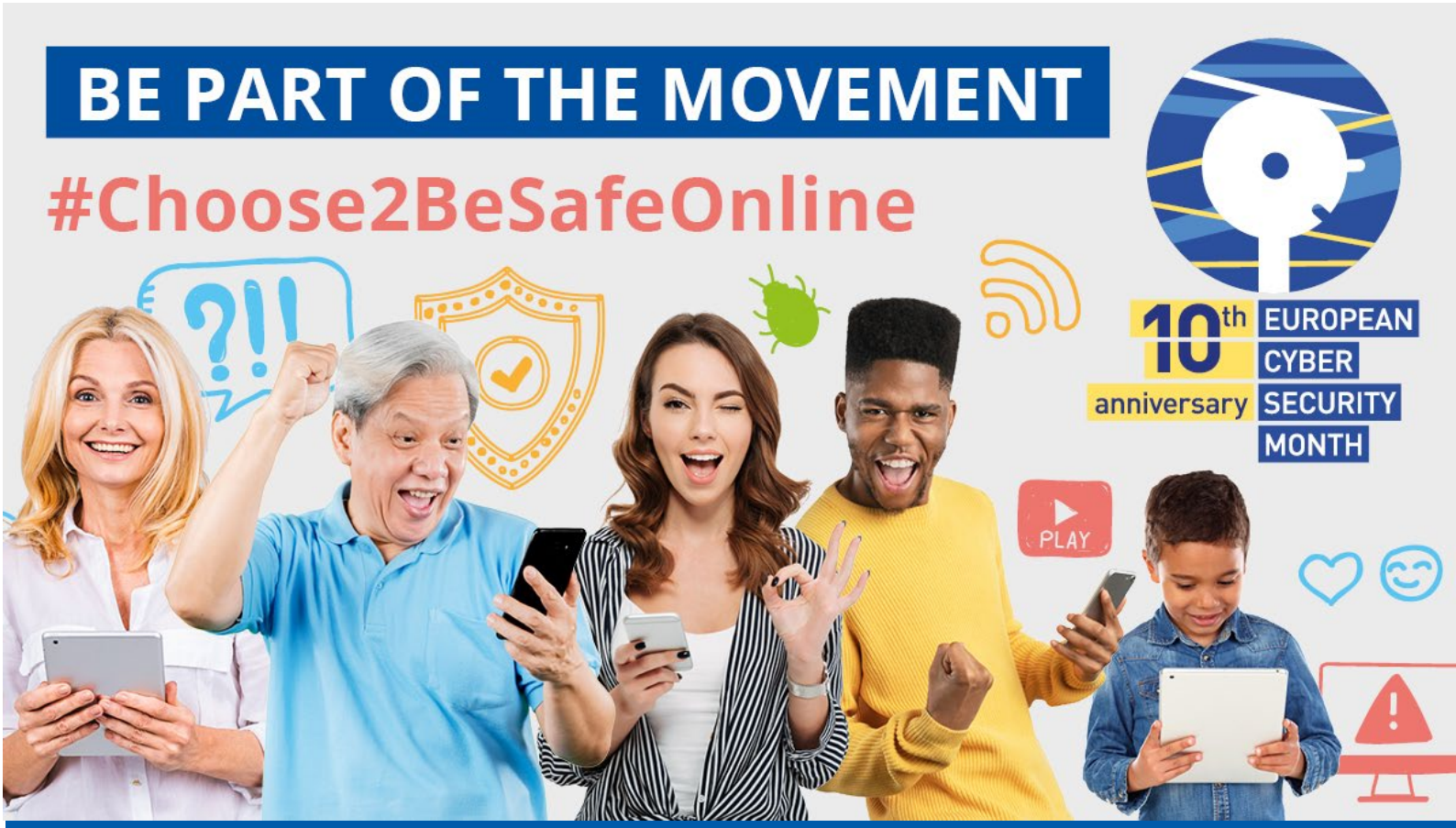
EUROPEAN UNION AGENCY
FOR CYBERSECURITY




# ECSM 2022 CAMPAIGN REPORT

European Cybersecurity Month (ECSM) 2022

MARCH 2023

# 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

## AUTHORS

Marianna Kalenti & Peter Biro, ENISA

## ACKNOWLEDGEMENTS

S2 Grupo, Kill Draper

## LEGAL NOTICE



## COPYRIGHT NOTICE



ISBN 978-92-9204-629-3, DOI 10.2824/36758

# EXECUTIVE SUMMARY

The fact that users are the first line of defence in the cybersecurity chain, has rendered the need for cyber awareness-raising imperative and, as a response to that the European Cybersecurity Month 2022 campaign focused on two of the most prominent threats:

1. **Phishing**: so that users may detect and react to the most common attack against individuals.
2. **Ransomware**: so that users become aware of the threat, learn how to identify it and react to it, and realise its severity by getting to know its consequences.

The target audience of the campaign, employees between 45-65 years old, was decided as an attempt to address the gap that exists between younger and older generations, as far as digitalisation is concerned, but also because ransomware is a predominant threat with great potential for damage to corporations.

What is more, the campaign was coupled with the commemoration of the ECSM's 10th anniversary in 2022, which was celebrated – among others – with the production of a "crowdsourcing" video that brought together the testimonies of people from all MS & organisations that have made the ECSM possible over the years.

The specifics of the campaign included **an additional motto "Choose To Be Safe Online"**, which was used, along with the existing ones, in order to convey the above. Several videos were produced for both themes, as it has been found that they have significant impact on the public and encourage the retention of ideas.

These were included in the landing pages created within the ECSM website for the two themes, along with a series of tips and informational data, presented in visual format, and a quiz that tested the knowledge that users acquired during the campaign.

For the ECSM 2022, an evaluation study with the inclusion of behavioural metrics was conducted in order to measure behaviour change. Surveys are seen as the most feasible ways to measure behavioural change (ENISA, 2021), supporting the notion that refocus of cybersecurity behaviour change evaluation should be directed towards behavioural metrics in surveys, which is a better measurement than compliance rates which merely indicate completion, not a long term, conscious effect on behaviour (Jacobs et al., 2022). Data collected after the campaign was compared to data from before the campaign, in order to assess the impact of the awareness raising attempts on cybersecurity behaviour. Successfully, data has shown a significant increase in self-reported cybersecurity behaviour post-campaign and among people who saw information related to the campaigns about the "Phishing" and "Ransomware" themes.

The campaign also had another profound impact, which extends towards perceptions of cybersecurity risks, attitudes towards cybersecurity, social norms around it and beliefs in control over users' appropriate responses to incidents which are all relevant aspects when aiming for cybersecurity behaviour change.

Some key findings of the campaign's evaluation and behavioural research were:

- MS participated broadly in the ECSM 2022 and provided positive feedback for the campaign.
- Dissemination of the campaign through social media was effective and a sustained growth of ENISA's social media reach was observed.
- Users interacted much more with the content compared to the interaction that resulted from the previous ECSM campaign. Furthermore, the ECSM 2022 generated a lot of interest outside Europe.
- The campaign had a positive impact on cybersecurity behaviour compliance, as people who saw the campaign report to perform cybersecurity behaviour more than those who did not.
- Data shows that all the cybersecurity behaviour types (related to email, password management, software updates, and network usage) have significantly increased in the target group after the campaign.
- Most participants claimed the campaign was easy to understand, although some said they were overwhelmed at first.

- The majority of people used the words “helpful”, “meaningful” and “informative” to describe the campaign and appreciated the applicableness of the offered guidance in avoiding the threats.
- Respondents did not feel that the campaign needed much improvement, they believed the content was fairly comprehensive and informative already, although participants suggested that it would be beneficial to include even more examples from the real world.

# TABLE OF CONTENTS

# 1. INTRODUCTION

## 1.1 THE ECSM STORY – CELEBRATING 10 YEARS OF CAMPAIGNS

The **European Union Agency for Cybersecurity (ENISA) and the European Commission** jointly coordinate the ECSM campaign every year, with the aim **to promote cybersecurity among European citizens and organisations** through awareness-raising activities and materials created specifically for this purpose.

**The European Union Agency for Cybersecurity (ENISA) and the European Commission jointly coordinate the ECSM campaign every year, with the aim** to promote cybersecurity among European citizens and organisations.

Supporting these campaigns are numerous **EU Member States** and **hundreds of different partners** (including governmental entities, universities, think tanks, NGOs, professional associations and private sector companies) from Europe and around the world.

The representatives of the Member States and the different partners function as **Ambassadors** of this campaign. Their mission is to **support and promote the campaign internally in their countries**. They complement their own national cybersecurity-related campaigns with all the materials, activities and events created by ENISA, thus making it easier for ECSM content to reach all EU countries in a way that is closer and more specific to the citizens of each one.

### 1.1.1 ECSM evolution through the years

In **2011**, the EU Agency for Cybersecurity was asked to study and assess the idea of creating a pan-European cybersecurity campaign for the Cybersecurity Month, October.

In **2012**, the ECSM pilot project was launched across Europe. It involved the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain, and the United Kingdom, where several events and activities took place. It was supported and endorsed by the EU Agency for Cybersecurity and the European Commission.

In **2013**, the ECSM aimed to increase the number of Member States involved, in order to focus on specific issues and start shaping the activities of this campaign across the European Union, which might have a global impact as well.

In **2014**, a total of 184 activities took place in 30 different countries, targeting different audiences such as employees, digital users, students, and IT experts, and focusing on different topics, including updates, privacy and encryption.

In **2015**, the number of activities reached more than 200 and two more countries joined the campaign. Activities were developed around the themes of cybersecurity culture, cloud solutions and the Digital Single Market.

In **2016**, ECSM activities doubled the ones of the previous year, all related to the themes of Cyber Security in Banking, Cyber Training, Cyber Safety and Mobile Malware.

In **2017**, the number of activities continued to grow from EU to EFTA countries, as 5 more countries joined, with the ECSM being represented in **37** different nations. The themes selected for that year were Cybersecurity in the Workplace, Governance, Privacy and Data Protection, Cybersecurity in the Home, and Skills in Cybersecurity.

Two countries dropped out in **2018**, when the themes were Cyber Hygiene, Digital Skills and Education, Recognize Cyberscams, and Emerging Technologies and Privacy. Another country joined again in **2019**, when Cyber Hygiene and Emerging Technologies were once more the themes.

COVID-19 burst into our lives in **2020**, forcing a change in the approach of the ECSM during that year. Thus, a very powerful campaign was created under the umbrella concept "Think Before You Click", which centred around Cyber scams and Digital Skills and achieved a much higher outreach than in previous years.

It is notable that, in **2021**, 73% of the Member States surveyed stated that the campaign had helped them reduce the number of cyber incidents. The campaign that year focused on the "Be Cyber Secure from Home" and "Cyber First Aid" themes (the first time that a theme focused on the aftermath of becoming a victim of a cyber-attack).

For the **2022** ECSM, the whole issue of cyber security at home, which was largely driven by the pandemic, was set aside to focus on the attacks themselves, with this year's themes being **phishing** (as the main entry vector exploited by cyber criminals when targeting people, rather than system vulnerabilities) and **ransomware** (as the most prolific and potentially damaging cyber-attack).


**Figure 1. 10th Anniversary Logo**

## 1.2 TARGET AUDIENCE OF THE 2022 CAMPAIGN

We live in a **hyper-connected society**, where digital transformation has been accelerated by the pandemic caused by Covid-19, and technological progress is rapid and unstoppable. These facts have given **cybercriminals a much larger attack surface**, therefore it is imperative that the European society is prepared to deal with such attacks.

**The main target audience of the Phishing campaign was people over 45 and up to 65 years of age, who are still employed**. These people's **everyday lives are largely digital**, as they generally use technology for their professional tasks, but also in their personal sphere, with mobile phones, tablets, smart devices, etc. This is coupled with **an expected low or limited level of knowledge of the cybersecurity domain** and, unfortunately, together these characteristics render them **an ideal target for cyberattacks**, as well as **the most easily exploitable entry vector** for larger-scale attacks.

In addition, in order to assure that the campaign would achieve to reach this type of audience, it was designed with a view to creating in them the feeling of "this could be me" and empowering their active involvement in cybersecurity, so that they would become **human firewalls for their organisations and homes.**

In the Ransomware behavioural-change campaign, the target audience was **45+ year-old employees of European companies and organisations**. Those are the most exploited entry points for cyberattacks, as they are unaware of the threats and seem used to delegating responsibility to the IT Department or higher. This is why the campaign was created in a simple and understandable language, in order to alert them to a plain message: **Anyone in your company could be hit by ransomware.**

The target audience of the **Phishing** campaign was **people over 45 and up to 65 years** of age, **who are still employed**.

The target audience for the **Ransomware** campaign was **45+** year old **employees** or European companies and organisations.

# 2. CAMPAIGN TARGET & CONTENT

## 2.1 ECSM 2022 VISION & OBJECTIVES

The mission of all entities that participated in ECSM 2022, was to establish a Cybersecure European space by raising awareness and providing EU citizens with tools and practical advice that would help them **adopt more cybersecure routines and become "Human Firewalls",** consequently boosting the resilience of their professional place as well.

The key objectives of the 2022 ECSM campaign were to:

- Raise cybersecurity awareness in the European Society and create a more secure European Cyberspace, among EU citizens and organisations.
- Create and disseminate awareness raising materials that provided the target audience with up-to-date online security information.
- Coordinate and conduct awareness raising activities and events.
- Encourage continuous behavioural change towards cybersecurity.
- Help reduce the occurrence of cybersecurity attacks, establishing users as elements of defence rather than vulnerabilities.
- Encourage the delivery of key awareness messages, via optimal channels, audio-visual designs and formats.
- Create engaging content on the chosen topics, suitable for the chosen target audience.
- Make use of efficient monitoring and evaluation mechanisms to assess campaign impact.
- Engage relevant stakeholders and increase the participation of EU Member States, European and International partners.
- Launch a pre and post-campaign research study in order to assess behavioural change in EU citizens' cybersecurity posture, as a result of the ECSM campaign.

## 2.2 ECSM AWARDS: A 2022 NOVELTY

In 2022, ENISA launched a joint action with the national ECSM Coordinators Group: the ECSM awards. The aim was, on the one hand, to increase visibility of the excellent and creative material the MS produced in the past years under the ECSM umbrella, and, on the other, to increase engagement and potential synergies.

MS representatives involved in the process are to vote every year for the most innovative and impressive materials produced for past ECSM campaigns. Thus, MS were asked to vote from a list of campaign material submitted to the competition.

The concept was piloted for the 1st time in 2022 and it came to stay. Member States' national coordinators were called to submit their candidatures and upload material on three categories:

- Best video
- Best infographic
- Best educational material.

In the **2022 ECSM Awards** Ireland won best infographic; Greece, best teaching material; Slovenia & Belgium, best video.

The winning material was translated in all EU languages and promoted anew within the year's campaign.

ENISA aims to organise this competition every year. The winners - which were announced by VIPs during the ECSM Campaign kick-off – were:

- **Best infographic:** Ireland: Become your own cyber security investigator, announced by European Commissioner **Johannes Hahn**
- **Best teaching material:** Greece: Treasure hunt games for primary school, announced by European Commission Director for Digital Society, Trust and Cybersecurity, **Lorena Boix Alonso**.

- **Best video:** Slovenia: Darko wants to take his girlfriend on a trip and Belgium: Passwords are a thing of the past. Protect your online accounts with two-factor-authentication, announced by ENISA Executive Director, **Juhan Lepassaar**.

## 2.3 ECSM 10TH ANNIVERSARY

2022 marked the ECSM's 10th year anniversary and special activities were put to place for its celebration.

Special activities were prepared for the **ECSM 10th Anniversary**

- **Anniversary-edition logo:** a 10th-anniversary badge was added to the ECSM logo and used in all material and activities of the year
- **Crowdsourcing video:** 19 MS-members of the ECSM Coordinators' Group, EUIBAs and the people who initiated the ECSM shared their stories and experience from the past 10 years in a potpourri video, which was aired during the ECSM Interinstitutional Launch event and promoted throughout October.
- **Thank-you bespoke gifts** and cards were created and sent to all contributing MS, EUIBAs & individuals.
- **Anniversary pop-up:** created for the ECSM website.
- **Interviews and articles** were delivered by ENISA on the ECSM story and mission.

# 3. CAMPAIGN DESIGN

The ECSM Coordinators' Group decided that the 2022 campaign would focus on **Phishing and Ransomware**, as they both are the most prolific threats in Europe and worldwide.

In order to maximize results and focus on the **audiences** that seem most vulnerable, it was decided that the campaigns would target people between **the ages of 45 and 65**. In particular, the Phishing campaign would focus more on the attacks that these people may suffer in their personal sphere and the Ransomware campaign on employees, as Ransomware is an attack much more directed towards companies.

To give the campaigns more "packaging", the (temporary) motto **"Choose To Be Safe Online"** was added to the other two ECSM slogans/hashtags, "**Think Before You Click**" and "**CyberSecMonth**".


**Figure 2. Motto Choose To Be Safe Online**

## 3.1 ECSM 2022 THEMES

### 3.1.1 Phishing

According to the ENISA Threat Landscape 2021[1], **phishing is the most commonly used attack**, on its own and as an entry vector for the perpetration of other, larger cyberattacks. It is so common that all of us have encountered it at numerous instances in our everyday lives. Moreover, it is a threat with a **wide variety of representation**, as it can be sent in numerous formats, such as email, instant messages, phone calls, or messages on other instant messaging platforms.

The ECSM 2022 Campaign focused on **Phishing** and **Ransomware**

**In 2021, the number of phishing attacks tripled, in comparison to the beginning of 2020, and in the first quarter of 2022 a new record was set, as it was the first quarter in which the number of phishing attacks exceeded one million** (at EU level). What is more, **phishing is responsible for 90% of data breaches** and the most common gateway used by cyber criminals to perpetrate other attacks of greater potential impact, such as ransomware.

### 3.1.2 Ransomware

The need for the creation of a communication campaign on ransomware lies in the fact that the **impact and consequences** of such attacks are very serious and sometimes even lead to the bankruptcy of companies. The threats posed by ransomware have continued to grow, advance and develop along with technology, and increasingly pose an even more sophisticated and damaging risk. In 2021 there was a **234% increase** of ransomware in Europe

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

and the **average downtime** after a ransomware attack is **21 days**. The theme was heavily related with the ENISA Ransomware Threat Landscape published in October 2021[2].

## 3.2 ECSM 2022 TARGET AUDIENCE PERSONAS

From the outset, it was clear that the campaign would focus on the so-called “digital immigrants". These are people who make extensive use of technology, but whose technology literacy is assumed and expected to be lower than that of the rest of the population. In addition, not many cybersecurity awareness campaigns focus on them, leaving them largely untouched.

It was therefore decided that the target audience for the phishing campaign would be the **population between 45-65 years of age**.

The target audience of the ransomware campaign would also be people 45 to 65, but this time **employees of European companies and large organisations**.

## 3.3 ECSM 2022 COMMUNICATION CHANNELS

**Various** communication channels were used for this ECSM campaign:

- **Landing pages** within the ECSM website for each of the campaigns, where all the materials produced were made available.
- The ECSM **website** (https://cybersecuritymonth.eu/) for the promotion of its 10th anniversary.
- Organic (Facebook & Twitter) and paid (Facebook, Twitter & YouTube) **social media posts** for the promotion of both campaigns and anniversary activities.
- A new **hashtag #Choose2BeSafeOnline** was added to the existing ones, in order to increase distribution potential.
- **All content** was created and produced in **English** and **subtitled in all EU official languages**, to increase the potential impact of the message in non-English-speaking countries.

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

# 4. CAMPAIGN EXECUTION

## 4.1 CONTENT CALENDAR

The campaign was structured around **a content calendar for social networks**, which was communicated to the MS prior to its start, so that they would also follow it alongside ENISA. The first half of October was dedicated to phishing and the second half to ransomware, with initial posts being made as follows and new content being published daily on all channels, afterwards.

- 21-28 September: teasers
- 30 September: pre-launch
- 1 October: launch alongside airing of the Anniversary Video
- 2 October: second launch posts.

## 4.2 LAUNCH OF THE ECSM 2022

On **Sep 27**, the European Cybersecurity Month kick-off event was organised by the EU Council, titled: **"A decade promoting cybersecurity awareness".** The event was structured around two sessions:

- **Growing ransomware trends: are the EU institutions ready?**

A high-level political debate on the impact of growing ransomware trends, the preparedness of the EU institutions, and the forthcoming Cybersecurity Regulation - against the background of increasing hybrid threats.

- **Cybersecurity awareness inside the EU institutions**

The debate on cybersecurity translates into concrete programmes for the EU institutions, bodies and agencies, as they aim to increase awareness among their staff. This session focused on testimonials and best practices with an aim to inspire organisations to up their game.

On **Sep 30** a Press release was published simultaneously across the EU, announcing the launch of the European Cybersecurity Month 2022 and the celebration of its 10th anniversary. Special video messages were delivered by EC officials: European Commission Vice-President for Promoting our European Way of Life Margaritis Schinas, European Commissioner for Competition Margrethe Vestager, European Commissioner for Internal Market and Services Thierry Breton, European Cabinet of Commissioner for Financial Budget Juhannes Hahn, Director for Digital Society, Trust and Cybersecurity in Directorate General for Communications Networks Content and Technology (DG CONNECT) Lorena Boix Alonso and ENISA Executive Director, Juhan Lepassaar, who also announced the winners of the ECSM Awards.

## 4.3 CAMPAIGN MATERIALS AND SOCIAL MEDIA CONTENT

ECSM 2022 materials were developed around the **"Choose to Be Safe Online" concept,** illustrated in the image of a shield that transforms into a human firewall,


**Figure 3. "Choose To Be Safe Online" concept**

and included the following:

- **Landing pages** were created on the ECSM website. They were used as platforms to deploy a story for each theme and included all related materials.
- **Social media images**: a series of social media posts and one accompanying video, images, and infographic.
- **Infographics**: three infographics per theme, providing insight to the current cybersecurity status in Europe.
- **Downloadable posters** raising awareness on the threats of phishing and ransomware. They were translated into 24 languages which resulted in a total of 150 versions in both PDF and editable, open format.
- **"Prevention Response for Ransomware Attacks" downloadable handbook**: a comprehensive document for managers of small and medium sized organizations to distribute to their employees and train them on how to prevent and deal with a ransomware attack.
- **Ambassadors' kit**.

Materials produced per theme:

- 1 main video
- 3 complementary videos (capsules)
- 3 illustrations with statistical data
- 8 illustrations with the main tips to protect oneself against phishing and ransomware
- 3 downloadable posters
- 3 Photos
- 1 quiz
- Infographics
- 1 post linking to the Cyber First Aid map.

Additionally, for the 10-year anniversary:

- A **14-minute video** was produced via crowdsourcing testimonials from Member States, EU Agencies and individuals who contributed to the ECSM over the years.
- A **10th-anniversary badge** was added to the ECSM logo.
- Special social media **posts**.
- Engraved **gift** and thank-you card.

# 5. CAMPAIGN EVALUATION

## 5.1 EVALUATION METHODOLOGY

The ECSM 2022 campaign was evaluated on the basis of the following:

- **Member State activities**: each Member State provided their campaign "history", including Partnerships and Ambassadors, target audience (if different from the general one), all national events and activities within the ECSM framework, material used, their own results and conclusions, etc.
- **ENISA central social media activities**: total number of mentions, total number of followers & their demographic data, top keywords, top hashtags, paid post results, etc.
- **ECSM Web Analytics**: number of visits, unique visitors, views, actions per visitor, time spent per visit, number of downloads,
- **Events**: time, place & theme of national events and activities within the ECSM.
- **Media monitoring**: each Member State provided statistics for all the channels or media used during their campaign.
- **Evaluation Questionnaire**: qualitative assessment of MS perceptions about the ECSM campaign.

## 5.2 MS QUESTIONNAIRE

Participating Member States were asked to fill-in an 11-question feedback survey as well as data reports, to improve European Cybersecurity Month efforts and coordination:

1. **How would you rate the overall implementation of the ECSM 2022 campaign? (scale 1-10)**
2. **Did ECSM 2022 support the outreach and promotion of your work in a satisfactory manner?**
3. **Did ECSM add value to your national campaign?**
4. **Did ECSM offer opportunities for improving your national campaigns through collaboration with other countries?**
5. **Do you think ENISA succeeded in sharing and promoting new ideas among ECSM partners?**
6. **Did the content (videos, infographics, GIFs etc.) produced by ENISA for the ECSM support your national campaign?**
7. **How would you rate the content produced for the ECSM 2022 campaign? (scale 1-10)**
8. **Could ENISA promote your awareness material better?**
9. **Do you think the ECSM offers opportunities for fostering a pan-European cybersecurity culture?**
10. **How would you rate the implementation of the ECSM 2022 by ENISA? (scale 1-10)**
11. **How likely are you to recommend partnering with ENISA on the ECSM next year to another organisation like yours on a scale from 1 to 10, where 1 is not at all likely and 10 is extremely likely?**

**Table 1. MS Questionnaire**

Overall, their responses yielded the following results:

1. The ECSM 2022 campaign was rated with an average of **7.5**.
2. **85,7%** MS state that the ECSM 2022 supported the outreach and promotion of their work.

3. **85%** MS believe that the ECSM added value to their national campaigns and that ENISA did a good job in promoting and sharing new ideas with its partners.
4. **75%** answered that the ECSM offered opportunities to improve their national campaigns.
5. **90%** stated that ENISA succeeded in promoting and sharing new ideas among ECSM partners.
6. **80%** indicated that the content created by ENISA for the ECSM supported their national campaigns.
7. The average content rate for the ECSM materials created by ENISA was **7,2**.
8. **100%** MS feel that ENISA offers opportunities for fostering a pan-European cybersecurity culture.
9. With the exception of 2 countries, all MS would recommend partnering with ENISA on ECSM next year.
10. The **net promoter** score was **38**.

**MS feedback for the ECSM 2022 Campaign was positive**, with most variables scoring above 80%

Additionally:

- **84% of MS** assess that the ECSM campaign had an **impact** on the reduction of cyber incidents.
- **The majority of MS** perceived that the **change in attitude** after the implementation of the ECSM campaign was more positive.
- Campaign's main strength: the **materials** created and the collaboration between the MS and ENISA.
- Campaign's main weakness: contents are very **concentrated** in October - users need more materials throughout the year.
- Average score of **7.1** for the effectiveness of the ECSM 2022 campaign to raise the belief that cybersecurity behaviours can actually prevent cybersecurity threats.
- Average score of **6.2** for campaign effectiveness in changing the perception that security compliance is a waste of time and not very productive.

## 5.3 ASSESMENT OF WEB RESULTS

### 5.3.1 ECSM website

The metrics indicate a very high level of awareness and that all objectives set for the period were met and exceeded.

**Users of the ECSM website interacted much more** with its content than previous year.

- **Visits to ECSM website increased** over the previous period by an average of **27%**, with the total visits being 31.8% more.
- **Visitors stayed 6.7% longer** on the ECSM website and the **bounce rate** was reduced by almost **12%**.
- **In October 2022, the ECSM website had 28.3% more page views than the monthly average of 2021.**
- **Downloads** of materials increased by almost **10%** and **out links** increased by **78%**.
- The most visits were made during weekdays.
- **76%** of the **traffic flow** to the ECSM website was generated by **social media posts** on Facebook, Twitter, LinkedIn and YouTube.
- ECSM website: **53% of users were redirected from Facebook, 10% from Twitter, 9.6% from LinkedIn, and 5.7% from YouTube**.

### 5.3.2 Cyber First Aid Map

The ECSM Cyber First Aid Map was included in this year's campaign too, as it provides users with information about the organisations to contact in case of a cyber incident, according to their geolocation. A link to the map was embedded in the landing pages for the two themes.

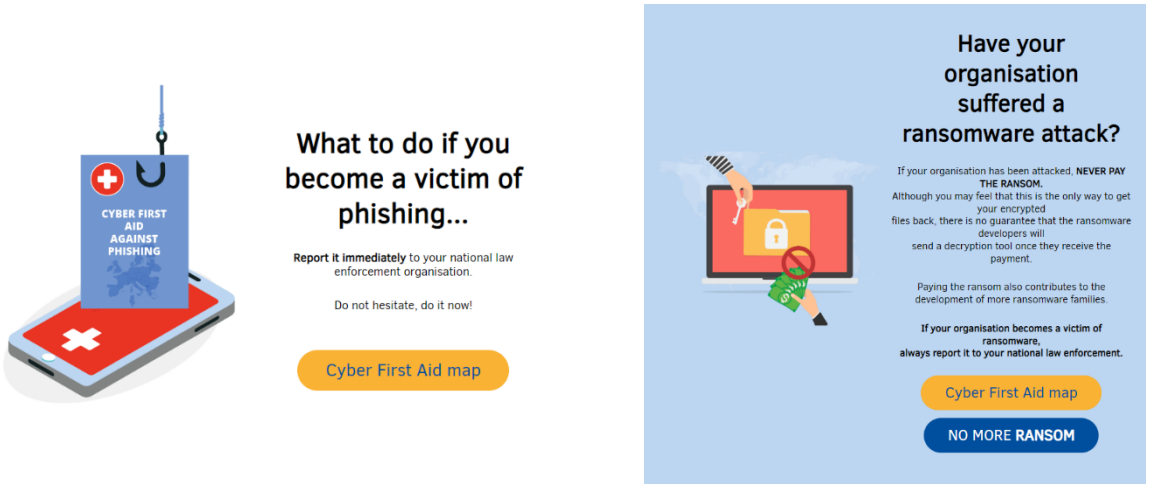



**Figure 4. Cyber First Aid Map link**

### 5.3.3 Media monitoring

To improve the impact on offline channels, a press release dedicated to the Ten Years of Raising Cyber Awareness Throughout Europe was published.

This press release had a significant impact in the media, owing to the use of hashtags dedicated to improving messages.

As a result, some **2,288** appearances in press media were found in the press clipping with a total daily audience of **675,155,981** readers. The impact in these media would have an advertising value of **7.5 million euros.**

More facts about the press release:

- **Keywords:**

A SEO strategy was set originally, containing the keywords below to undermine the text:

- European Cybersecurity Month
- #CyberSecMonth
- #ThinkB4UClick
- #Choose2BeSafeOnline
- ENISA

- **Period:**

The analysis period used for the follow-up of the press release was approximately two months. It was not limited to October, i.e. the period immediately after its release but stretched to November as well. With this technique, it was possible to find a correlation between the increase in the organisation's shares and the exposure of the press release on the European Cybersecurity Month website.

- **Territories:**

The following countries were analysed: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

- **Press Sentiment:**

According to the subject matter of the content and the algorithm's capacity to identify details of tone, **947 posts were identified as positive tone, 1125 were identified as neutral tone and 141 were negative.**

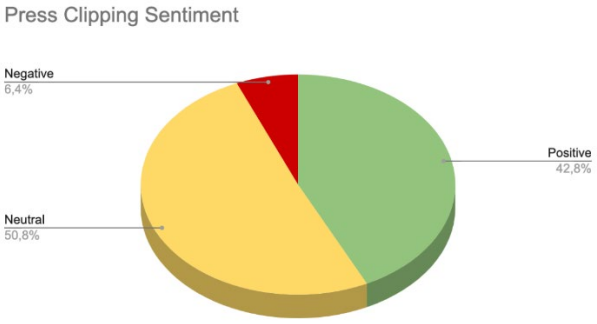



**Figure 5. Press Clipping Sentiment**

- **Keywords' Distribution**

The keywords were distributed as follows:

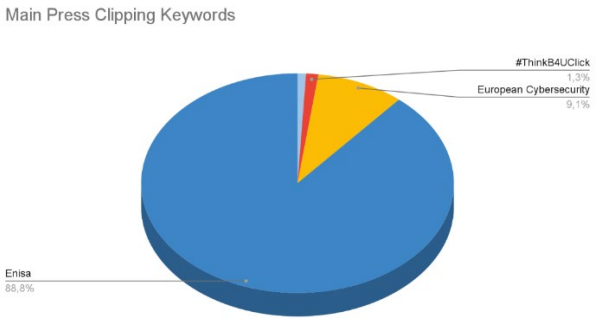



**Figure 6. Main Press Clipping Keywords**

### 5.3.4 Social media

**ECSM 2022** campaign content was published through organic and paid media, and on three social media platforms, Twitter, Facebook and YouTube.

Noteworthy findings include the following:

- Overall activity came from **many different countries**.
- The **total follower growth** achieved by ENISA, from 2021 to 2022, was **9.6% for Twitter** and **16% for Facebook**.
- Total Reach: despite having less visibility, 2022 content achieved greater user engagement.
- **Interaction on Twitter was consistently higher than on Facebook in volume**.
- The platform with the lowest number of interactions in the form of "likes" was YouTube.
- Interactions with the content were higher during weekdays than in the weekend.
- #CyberSecMonth hashtag appeared to be the most represented.
- Most Twitter users (11K) were located or based in European countries.
- A big number of users who interacted with the website were based in the United States.
- A total of **4K users interacted with the web pages**.

A **sustained growth on social media** was observed throughout the campaign

- Trend topics


**Figure 7. Trend topics**

- **Paid posts:**

– Higher granularity led to higher results, compared to ECSM 2021 (i.e., this year different campaigns were created, one for content, one for videos & one for each country).
– Campaign total: **18,142,291 impressions**, on all social networks.
– **Five times more views** achieved for the content on social networks, reaching a total of **5,913,475 views**.
– **47,892 total social media clicks** = more people came to the website redirected from social media (vs accessing it directly).
– Users **stayed longer** on the website and **interacted more** with the content than last year.
–


**Figure 8. Social Media Views & Clicks**

- **Campaign Audience:**

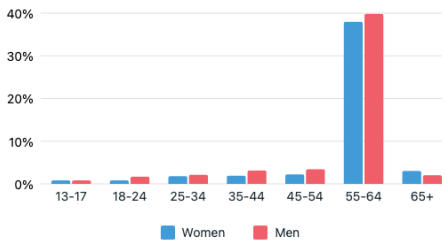



**Figure 9. Campaign Audience**

## 5.4 BEHAVIOURAL CHANGE ANALYSIS

In the context of the ECSM 2022 campaign, ENISA launched, for the first time, a pre and post campaign survey to measure the resulting behavioural change and impact. In brief, the following results and recommendations were drawn from the study:

**Results**

- The studied sample reported higher engagement in cybersecurity behaviour (self-reported cybersecurity behaviour) after the campaign, than that reported by the sample before the campaign.
- Respondents who declared to have seen information related to the campaign's themes were observed to score higher on cybersecurity behaviour score than respondents in the pre-campaign phase.
- The higher the intentions towards performing cybersecurity behaviour, the more likely people are to perform it.
- In order to increase vulnerability, it is important to increase awareness about cyber threats and focus on the efficacy of users' actions.
- When people think that performing appropriate security behaviours to protect their data is a good idea, a necessity or beneficial, this translates into a willingness to perform the behaviour and, in the end, to execute it.
- When respondents believed that their immediate environment - such as friends, family, colleagues and managers - think they should follow cybersecurity guidelines, it makes them more likely to adhere to them.
- Performing cybersecurity behaviour compliant with guidelines depends on people's perceptions of cybersecurity.
- People's perception of how effectively a response can prevent a threat and their confidence in their skills greatly contributes to the willingness to perform cybersecurity behaviour.
- Normative beliefs were found to be a key factor for cybersecurity behaviour.
- The campaign's target audience - people over 45 years old – were observed to be significantly more likely to perform cybersecurity behaviour compared to younger people.
- Cybersecurity behaviour was observed to vary depending on occupation.
- Overall, participants indicated that the campaigns helped protect them from "Phishing" slightly more than "Ransomware".

# 6. CONCLUSIONS & RECOMMENDATIONS

Upon analysis of the results presented above, the following conclusions were drawn for the ECSM 2022 Campaign.

Of the countries that responded to the survey:

- MS participated broadly in the ECSM, by sharing content and organising different activities.
- Overall feedback from MS was positive, with most variables scoring above **80%**.
- **Short videos** were the type of material that generated the most views and user interactions.
- Users of the ECSM website **interacted much more** with its content, therefore it is deemed that the target audience was reached more efficiently.

Regarding social media:

- A sustained growth was observed throughout the campaign.
- Most of the people who accessed the ECSM website were redirected from the social networks. Therefore, it is considered that dissemination through social media was effective.
- The target audience that was receptive to the messages on the social networks was likewise responsive to the contents of the website.

Finally, the findings of the behavioural study indicated the factors on which awareness campaigns should forcus, in order to result in far-reaching cybersecurity behaviour compliance:

- Inform and inspire audiences by providing real-world examples and illustrating the way cyber threats can affect them, as this helps them understand better and endure being careful and alert in the future.
- Provide practical, concise, and easy to execute instructions and advice that individuals can apply in their interactions with software, networks, and information infrastructures.
- Facilitate discussion and sharing of information with others, as it was found that nationwide and international campaigns influence the behavior of indivduals but also of people in organisations.
- Consider various constructs related to cybersecurity behaviour, when designing campaign and awareness communication, for a comprehensive influence and profound impact.
- Critical investigation needs to be undertaken, at an organisational and national level, to understand barriers to motivation, e.g., organisational or technological issues, as well as the level of security culture and risk of insider threat.
- When designing campaigns for behaviour change, one must consider the indirect effects of the campaign occurring through word of mouth, as well as the measurable self-reported individual behaviour.

None of above factors is sufficient by itself, but their combination can facilitate effective targeting.

# ANNEX

## 1. ENISA PROMOTIONAL MATERIAL:

All material for both campaigns can be found here:

| ENISA Promotional Material | |
|---|---|
| **General** | https://cybersecuritymonth.eu/ |
| **Phishing Campaign** | https://cybersecuritymonth.eu/phishing |
| **Ransomware Campaign** | https://cybersecuritymonth.eu/ransomware |

**Table 2. ENISA Promotional Material**

## 2. VISITS OVER TIME:


**Figure 10. Visits over time**

## 3. GEOGRAPHIC DISTRIBUTION

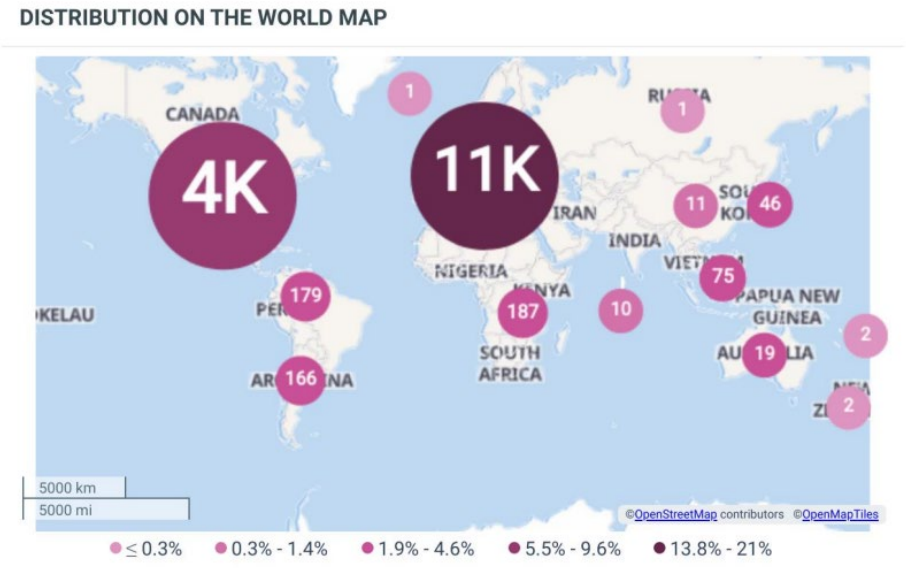



**Figure 11. Geographic distribution**

TP-05-23-086-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 978-92-9204-629-3
DOI 10.2824/36758