



ECSM 2023 CAMPAIGN REPORT

APRIL 2024

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 ehealthSecurity@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

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), 2024

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".

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 978-92-9204-665-1 DOI 10.2824/005990



TABLE OF CONTENTS

1. INTRODUCTION	5
1.1 COMMUNICATION PLAN & DEPLOYMENT	5
1.2 CONTENT CREATION	5
1.3 INTERACTIVE ENGAGEMENT	5
1.4 YEAR-ROUND CAMPAIGN	5
2. CAMPAIGN OVERVIEW	6
2.1 CREATIVE UMBRELLA: "BE SMARTER THAN A HACKER"	6
2.2 CAMPAIGN ACTIVITIES AND PERFORMANCE	6
2.3 TARGET GROUP AND CHANNELS	6
2.3.1 Target Group	6
2.3.2 Campaign Promotion Channels	6
2.3.3 Impact Assessment and Feedback Collection	7
2.4 MAIN CREATIVE AWARENESS SONG	7
2.4.1 Collaborative Creation Process	7
2.4.2 Impact and Engagement	7
3. CAMPAIGN MIX	8
3.1 UMBRELLA CONCEPT: "BE SMARTER THAN A HACKER"	8
3.2 WEBSITE LANDING	8
3.3 RED FLAG VIDEOS	9
3.4 CAMPAIGN CONTENT CALENDAR	10
3.5 DOWNLOADABLE POSTER	10
3.6 CYBERCRIMINAL PROFILE VIDEO	11
3.7 INFOGRAPHIC	12
3.8 SOCIAL MEDIA IMAGES	12
3.9 HELPFUL TIPS	13
3.10 QUIZ TIME	13



3.11	ECSM AWARDS	14
4.	ECSM IN NUMBERS	15
4.1	ENGAGING COMMUNICATION MIX	15
4.2	ENGAGING MEMBER STATES	24
5.	CONCLUSIONS & RECOMMENDATIONS	28



EXECUTIVE SUMMARY

European Cybersecurity Month (ECSM) 2023 took a different approach than in 2022. ENISA decided to take cybersecurity awareness to a different level, transforming the original ECSM campaign, which used to take place only during October, into a yearlong communication plan and strategy.

The 2023 ECSM celebrated cybersecurity and awareness throughout the entire year. To do so, ENISA worked together with the Coordinators' Group to decide on the road map for the new strategy. Several meetings took place, and the Annual plan was decided. Various mini campaigns were launched during the year, coinciding with special commemorative days related to cybersecurity. In addition, October took most of the focus, with numerous videos, illustrations, etc., which were tailor-made and produced to target the 2023 topics and audiences.

Also in cooperation with the Coordinators' Group, it was determined that the 2023 campaign should focus on Social Engineering for the general public. Once the decision was made, ENISA started working on a communication plan and ideas for the deliverables.

Overall, and even though ENISA's ECSM 2023 campaign did not include paid media and relied only on organic posts, the results exceeded expectations and achieved the desired objectives. The overall performance yielded better numbers than past campaigns, which, by contrast, did employ paid social media.

Posts reached the target audience, raising awareness about the risks of social engineering for the general public. Contents (particularly photographs, which performed better than other formats) generated interest and engaged the audience attracting new followers on ENISA's social media profiles, potentiating its media presence.

The ECSM 2023 focused on Social Engineering and was aimed at the general public.



1. INTRODUCTION

The European Cybersecurity Month (ECSM) 2023 took place throughout the entire year and focused most of its efforts in October. The campaign commenced on the 1st and spanned the entire month, concluding on the 31st. This year's central theme focused on the critical subject of Social Engineering. The campaign strategy integrated various communication methods, educational materials, interactive quizzes, and downloadable resources across multiple social media platforms including Facebook, Instagram, and Twitter.

1.1 COMMUNICATION PLAN & DEPLOYMENT

- Developed a comprehensive communication strategy tailored to the theme of Social Engineering.
- Utilised diverse communication channels such as original video content, website design, image-based educational materials, videos, quizzes, and downloadable resources.
- Targeted dissemination across Facebook, Instagram, and Twitter throughout the month of October to reach a broad audience.

1.2 CONTENT CREATION

- Produced an original video to enhance engagement and disseminate essential cybersecurity insights.
- Designed an intuitive website interface to provide centralised access to educational materials and resources.
- Created a range of visually appealing educational materials, including images and videos, to convey cybersecurity awareness effectively.

1.3 INTERACTIVE ENGAGEMENT

- Developed an awareness-raising quiz to engage the audience and promote understanding of cybersecurity threats and best practices.
- Offered downloadable resources to encourage continued learning beyond the campaign period.

1.4 YEAR-ROUND CAMPAIGN

In addition to the month-long ECSM campaign, a year-round initiative was introduced. This ongoing effort included themed campaigns tailored for each month, catering to various cybersecurity aspects and broader digital safety concerns:

- **Internet Day:** Highlighted the significance of safe and responsible internet usage.
- **Data Protection Day:** Focused on the importance of safeguarding sensitive data.
- **Backup Day:** Emphasised the necessity of regular data backups for protection against cyber threats.
- **World Password Day:** Raised awareness about strong password creation and management.
- **World Social Media Day:** Advocated for safe and responsible social media practices.
- **Sys Admin Day:** Acknowledged the crucial role of system administrators in maintaining cybersecurity.
- **Summer Tips:** Offered specific cybersecurity tips tailored for the summer season.
- **Black Friday:** Alerted users about potential cyber threats during high-traffic shopping events.
- **Health:** Highlighted cybersecurity aspects related to healthcare data protection and privacy.

The ECSM 2023 took cybersecurity awareness to a new level, expanding the scope of the campaign to the entire year.



2. CAMPAIGN OVERVIEW

2.1 CREATIVE UMBRELLA: "BE SMARTER THAN A HACKER"

The campaign's creative umbrella, "Be Smarter than a Hacker," serves as a powerful reminder emphasising the significance of vigilance and discernment while engaging online. This claim effectively resonates due to several key reasons:

- **Awareness of the Threat:** It amplifies the understanding of the omnipresent threat posed by hackers and social engineering tactics. This heightened awareness is crucial for individuals to recognise potential risks.
- **Personal Empowerment:** The claim instils a sense of personal empowerment, emphasising that individuals possess the capability to protect themselves by being vigilant and informed in their online interactions.
- **Encouragement of Caution:** It promotes a cautious mindset, encouraging individuals to exercise prudence and critical thinking, thus reducing susceptibility to social engineering tactics.
- **Promotion of Education and Awareness:** By fostering a culture of education and awareness, the claim encourages continuous learning and knowledge acquisition in cybersecurity matters.

"Be Smarter than a Hacker" serves as an effective rallying cry against social engineering techniques. It motivates individuals to exercise caution, empowers them to take control of their online interactions, and emphasises the ongoing importance of education and awareness in combating cyber threats.

2.2 CAMPAIGN ACTIVITIES AND PERFORMANCE

The campaign activities implemented during the ECSM encompassed a range of content formats tailored to engage and educate audiences across Europe. This report will delve into the specifics of each activity, evaluating their individual performance and impact in raising cybersecurity awareness among the targeted demographic.

2.3 TARGET GROUP AND CHANNELS

2.3.1 Target Group

The European Cybersecurity Month (ECSM) campaign aligned with expectations, targeting the general public with a deliberate focus on ensuring inclusivity and relevance across diverse demographics.

2.3.2 Campaign Promotion Channels

Social Media Engagement: Leveraged popular social media platforms including Facebook, Instagram, and Twitter to disseminate campaign content. These channels facilitated widespread outreach, engaging audiences across varied age groups and interests.

Online Survey Distribution: Deployed an online survey that was distributed among Member States to gather valuable insights and feedback. This approach allowed for the collection of diverse perspectives and opinions, enhancing the campaign's adaptability and relevance.



2.3.3 Impact Assessment and Feedback Collection

The utilisation of social media channels enabled a broad reach and engagement across different demographics, ensuring the campaign's message reached a wide audience.

The inclusion of an online survey distributed among Member States was a proactive measure to gather feedback, perceptions, and experiences regarding cybersecurity awareness. This feedback loop provided valuable insights for future campaign improvements and content refinement.

The campaign's strategic choice of targeting the general public along through social media platforms and online surveys showcases a commitment to inclusivity and comprehensive engagement. The data collected through these channels will be instrumental in assessing the campaign's effectiveness and tailoring future initiatives for heightened impact.

2.4 MAIN CREATIVE AWARENESS SONG

For the European Cybersecurity Month (ECSM) campaign, a strategic decision was made to cater to a diverse target group by creating a unifying musical piece accessible to all audiences. To achieve this, a contest was initiated involving six different musicians representing varied musical styles ranging from folk, Afro, indie, to big band.

2.4.1 Collaborative Creation Process

Contest and Musical Diversity: The contest facilitated collaboration with musicians spanning diverse genres, ensuring representation across a broad spectrum of musical tastes and preferences. This approach aimed to resonate with a wide range of audience demographics.

Global Collaboration: Musicians from around the world came together, contributing their unique styles and cultural influences. This global collaboration not only diversified the musical composition but also promoted a sense of inclusivity and unity across borders.

Musical Video Clip Creation: Through this collaborative effort, a main song was composed, incorporating elements from various musical styles into a cohesive musical piece. This main song served as the centrepiece for a visually engaging musical video clip, combining creativity, diversity, and cybersecurity awareness messaging.

2.4.2 Impact and Engagement

The collaborative creation of the main song provided to the diverse tastes and preferences of the ECSM campaign's wide-ranging target audience, ensuring resonance with various demographic groups.

By fusing multiple musical styles into a unified piece, the campaign aimed to capture attention and engage audiences through a creative and memorable musical experience, enhancing the overall impact of the cybersecurity awareness message.

The creation of a collaborative song involving musicians from different genres and regions demonstrates an innovative and inclusive approach to engaging diverse audiences. This musical endeavour aimed not only to raise awareness about cybersecurity but also to connect with individuals on a universal and emotional level through the medium of music.

For the ECSM 2023 we created an awareness song about Social Engineering threats using our main umbrella concept “**Be Smarter than a Hacker**” to better impact and engage the targeted public



3. CAMPAIGN MIX

Consult entire campaign here: <https://cybersecuritymonth.eu/smarterthanahacker>

3.1 UMBRELLA CONCEPT: "BE SMARTER THAN A HACKER"

To anchor efforts in raising awareness about social engineering, the ECSM centred its campaign on the concept of "Be Smarter than a Hacker." This thematic core was visually represented by a clever thinking bubble image, designed to be both witty and insightful.



Illustration 1. 2023's ECSM campaign logo

3.2 WEBSITE LANDING

To broaden the dissemination of the message, ENISA strategically employed a [landing page](#) as the central platform for the narrative deployment. This accurately crafted landing page served as a gateway for users, granting access to a compelling array of content, including four original musical videos, a comprehensive series of tips and tricks to identify social engineering, downloadable posters, an interactive quiz to gauge individual knowledge levels, and facilitated access to a cybersecurity kit.

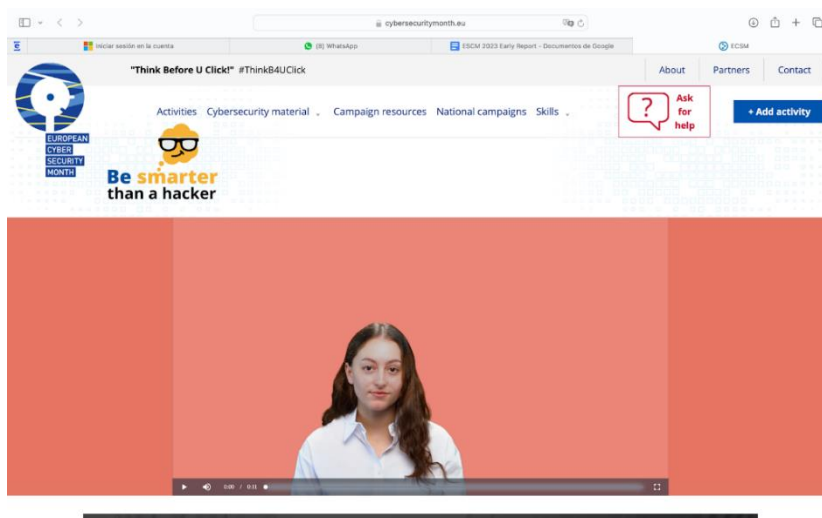


Illustration 2. 2023's ECSM campaign landing page

3.3 RED FLAG VIDEOS

ENISA developed three distinct red flag videos specifically designed to highlight key indicators of social engineering tactics. These videos were focused on recognising and addressing unexpected requests, unbelievable offers, and urgency—key elements that often signal potential social engineering attempts.

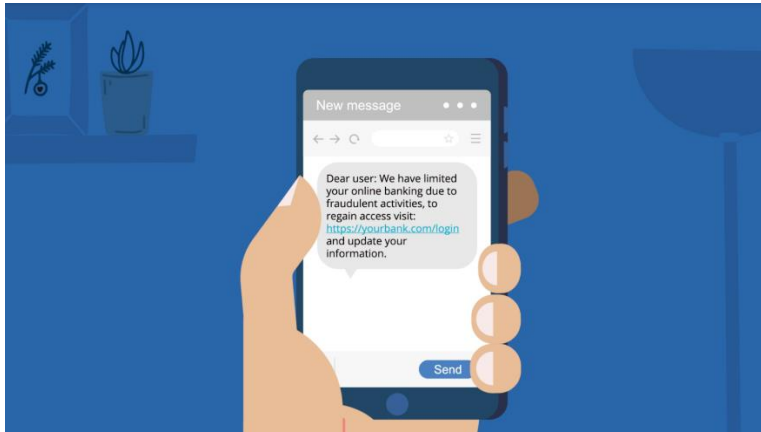


Illustration 3. 2023's ECSM campaign Red Flag Video: Unexpected requests

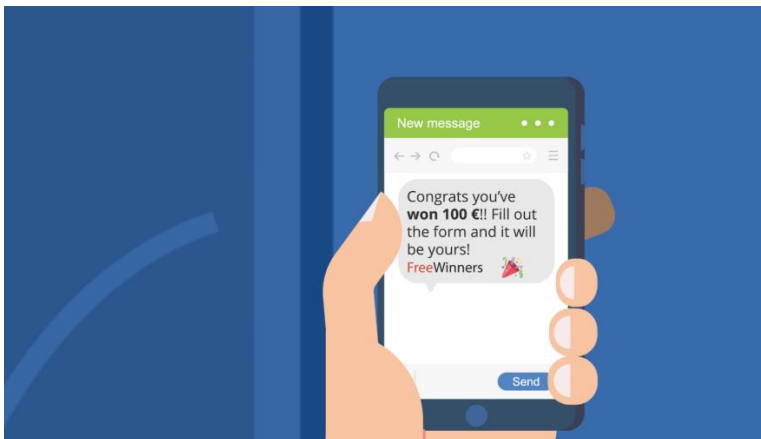


Illustration 4. 2023's ECSM campaign Red Flag Video: Unbelievable offers

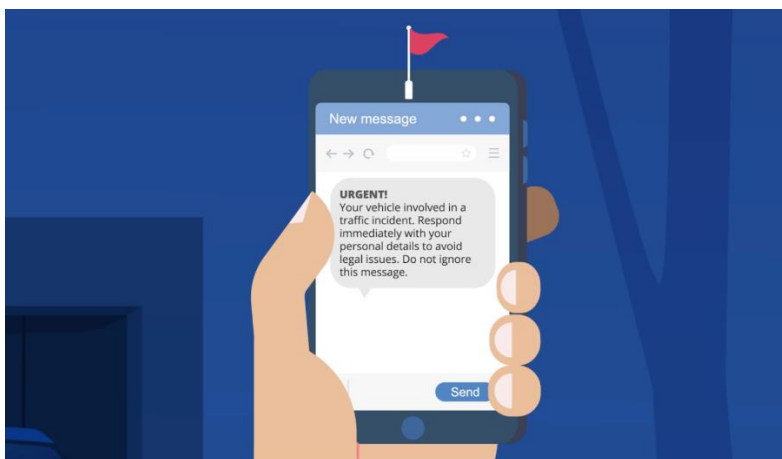


Illustration 5. 2023's ECSM campaign Red Flag Video: Urgency

3.4 CAMPAIGN CONTENT CALENDAR

The campaign was precisely organised using a [content calendar](#) tailored for social networks. This structured approach ensured a comprehensive presentation of social engineering topics alongside educational videos, crucial tips, downloadable materials, engaging quizzes, and more. This strategic scheduling optimised the delivery of diverse and informative content to our audience across various social media platforms.

The Open ECSM sub-campaign was an initiative that urged individuals to actively participate by sharing their own experiences and insights related to social engineering on their personal social media channels. This engagement-driven sub-campaign aimed to foster a community-driven dialogue, encouraging the sharing of valuable knowledge and personal encounters with social engineering tactics among peers and networks.

The year-round campaign was meticulously structured around a series of diverse themes spanning the calendar year. Each month was dedicated to a specific theme aimed at addressing various aspects of cybersecurity and digital safety. These themes included Internet Day, Data Protection Day, Backup Day, World Password Day, World Social Media Day, Sys Admin Day, Summer Tips, Black Friday, and Health. This strategic approach allowed for a continuous and targeted focus on different facets of cybersecurity, ensuring a sustained and comprehensive awareness effort throughout the year.

3.5 DOWNLOADABLE POSTER

The downloadable poster serves as a vital tool in raising awareness about the often-overlooked threats posed by social engineering. Crafted to inform and educate, these posters are available in both original PDF formats and editable open formats. It aims to enlighten individuals about the subtleties of social engineering tactics, empowering them with knowledge and actionable insights to better safeguard themselves against potential cyber threats.

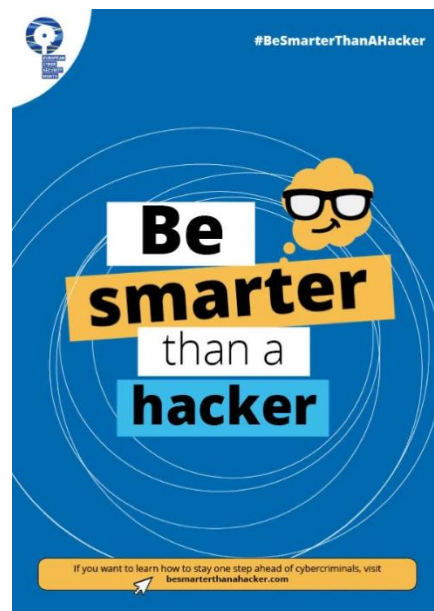


Illustration 6. 2023's ECSM campaign downloadable poster

3.6 CYBERCRIMINAL PROFILE VIDEO

The animated video was carefully created to illuminate the profile of social engineering criminals. This engaging and informative video utilised animation to vividly portray the characteristics and behaviours of cybercriminals employing social engineering tactics. Its primary focus was on educating viewers about the key identifiers and traits associated with these deceptive individuals, empowering the audience to recognise and guard against potential threats posed by such cybercriminals.

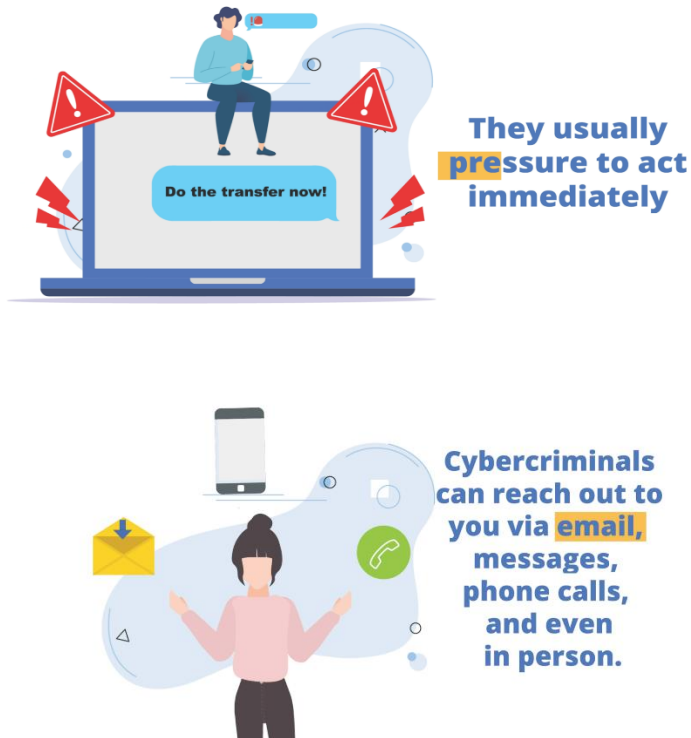


Illustration 7. 2023's ECSM campaign cybercriminal profile video

3.7 INFOGRAPHIC

The creation of two impactful infographics on social engineering was aimed at raising awareness and highlighting the severity of these threats. These visually engaging infographics incorporated updated data, offering a comprehensive snapshot of the current cybersecurity landscape in Europe. Designed to serve as informative resources, they provide valuable insights for anyone seeking a deeper understanding of social engineering, contributing to a broader knowledge base on this critical cybersecurity topic.

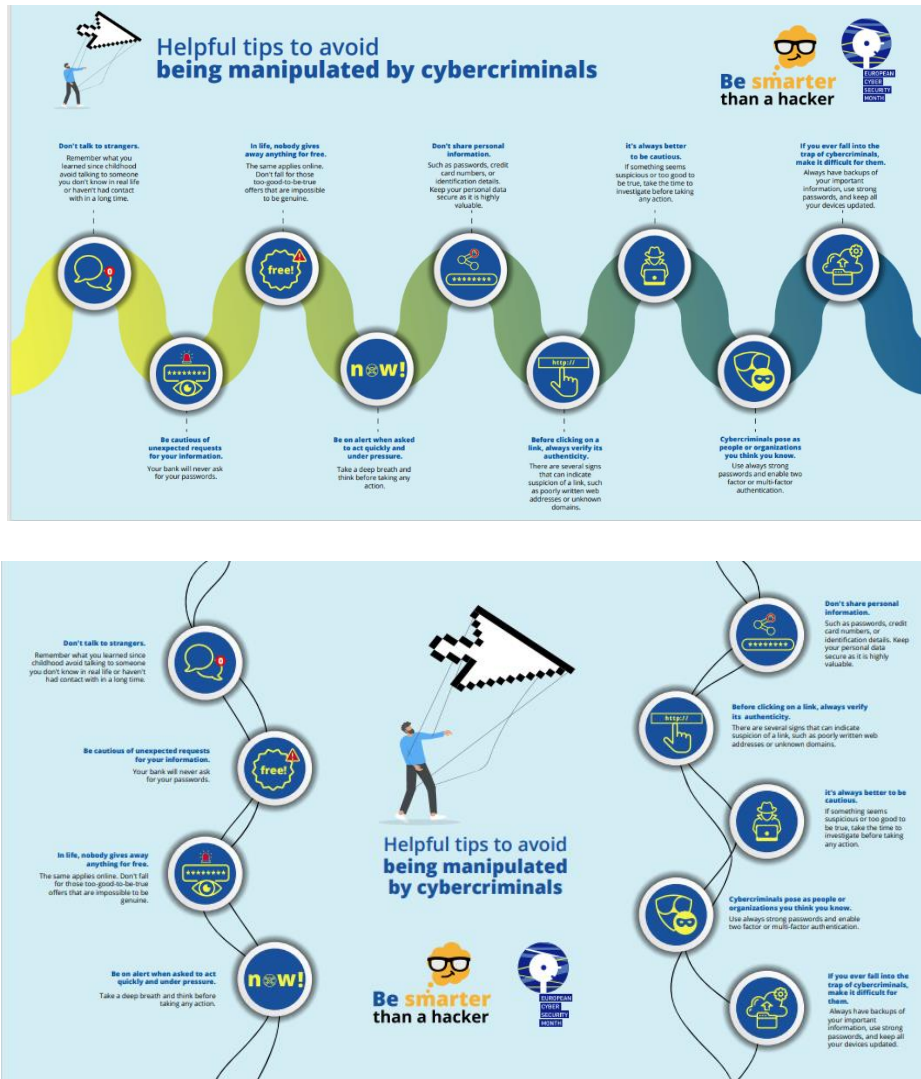


Illustration 8. 2023's ECSM campaign infographics

3.8 SOCIAL MEDIA IMAGES

The campaign encompasses a diverse array of engaging content customised for social media platforms, including a compelling video, visually captivating images, and an informative infographic. These thoroughly crafted materials are strategically organised to encourage active participation in the European Cybersecurity Month campaign. Their purpose is to spark interest, stimulate discussions, and motivate individuals to get involved in promoting cybersecurity awareness throughout the month.

3.9 HELPFUL TIPS

The initiative included the development of a set of ten valuable tips specifically aimed at aiding individuals in identifying social engineering tactics. These curated tips were designed to equip the audience with practical knowledge and actionable guidance, empowering them to recognise and thwart potential social engineering attempts effectively.



Illustration 9. 2023's ECSM campaign tips

3.10 QUIZ TIME

The creation of a simulated social engineering email attack served as an interactive and educational quiz designed to evaluate the cybersecurity preparedness of the target audience of the ECSM campaign. This simulation provided a hands-on experience, allowing individuals to gauge their ability to identify and respond to potential social engineering email attacks, ultimately enhancing their cybersecurity awareness and preparedness.

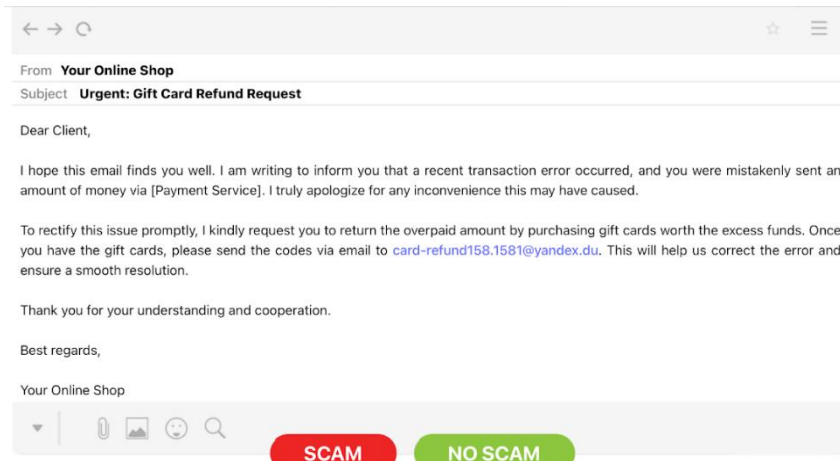


Illustration 10. 2023's ECSM campaign quiz

3.11 ECSM AWARDS

During the ECSM 2023 campaign, the ECSM Awards ceremony unfolded, showcasing excellence in three distinct categories: Video, Educational Material, and Infographics.

The Awards video segment was streamed online, featuring precisely recorded and edited content. The finalised video was strategically launched on the day of the event, accompanied by a well-crafted press release for widespread dissemination.



Illustration 11. 2023's Awards Ceremony

4. ECSM IN NUMBERS

4.1 ENGAGING COMMUNICATION MIX

The communication mix for the European Cybersecurity Month (ECSM) 2023 campaign did not employ any paid social media, therefore it had to rely only on organic posts. Thus, the ECSM 2023 was strategically crafted to overcome this fact and embody traits of engagement, boldness, and playfulness. This deliberate approach aimed to provoke contemplation and discussion about the critical digital security issue of social engineering.

ECSM 2023 in numbers		
Quantity	Description	Category
1	Social Media Content Calendar	SM Calendar
78	Days of campaign	SM Calendar
97	Original Content	SM Calendar
27	Mini Campaigns content	SM Calendar
45	October campaign content	SM Calendar
6	Initial Song Challenge	SM Calendar
1	Final Mastered HiFi Song	Video
1	Main Social Engineering Videoclip	Video
3	Red Flag Awareness Video	Video
1	Cybercriminal Profile Video	Video
1	Awards Event	Video
1	Campaign Poster	Downloads
2	Social Engineering Infographics	Downloads
1	Ambassadors Kit	Downloads
1	Main Landing Page	Web
1	Educational Quiza	Web
212	Posts Across Networks	Social Media
1	Social Media Management	Social Media
1	Twitter Engagement Video Campaign	Social Media

Table 1. ECSM 2023 in numbers

The ECSM 2023 campaign has introduced, as mentioned earlier, the innovation of distributing posts throughout the entire year, logically increasing the number of publications in October in line with the observance of Cybersecurity Awareness Month.

Upon a comprehensive analysis of the results from all the posts made across various platforms or social media throughout this year, it is observed that the content has been displayed 134k times. Out of these instances, 104k users have effectively viewed these posts. Furthermore, more than 2k interactions have taken place with the content, including sharing, liking, or reacting to the posts.

The ECSM 2023 campaign content was effectively viewed by 104k users.

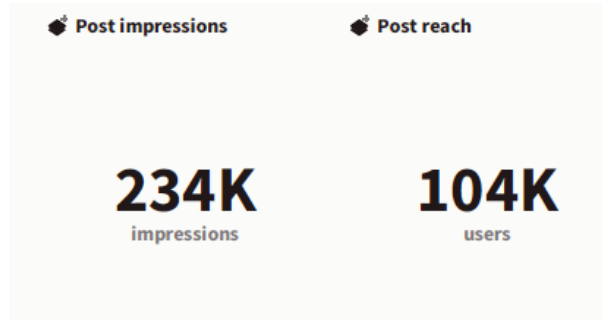


Figure 1. Posts impressions and reach

If we examine the number of posts made on different platforms, the following is evident. Facebook has been the most utilised social media platform, with 112 posts. This is followed by Instagram with 69 posts, and Twitter with 35.

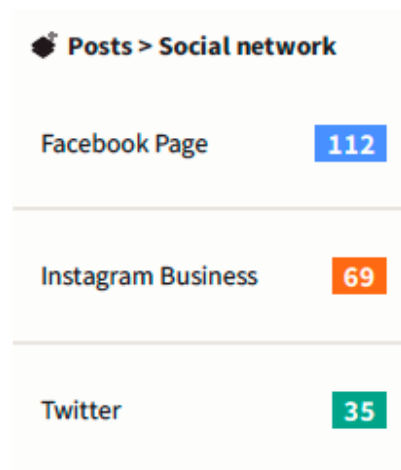


Figure 2. Number of posts on each social media channel

Twitter, being the social media platform with the uppermost number of followers, has generated the highest number of impressions despite sharing the least content. Specifically, the content posted on Twitter has been displayed 129K times, 1.25 times more than on Facebook and 58.64 times more than on Instagram.

However, the number of reactions and likes, which could be considered as a benchmark for calculating real user engagement with the content, has not shown as much disparity across Twitter and the other platforms. In fact, Facebook has achieved 1.57 times more reactions and likes (with a total count of 804) than Twitter (with a total count of 512) (the reasons for this difference will be analysed below).

Facebook has also garnered a very high number of impressions. When comparing the significant difference in the number of followers between Twitter and Facebook—almost 17 times more followers on Twitter than on Facebook (with Twitter having 32K and

Facebook 1.9K followers)—it is noteworthy that the number of impressions is not as disparate (1.25 times more on Twitter than on Facebook), with Twitter obtaining 129K impressions and Facebook locating 103K.

This could be attributed to various factors. Certainly, the difference in the number of posts made on each platform has influenced this outcome (with a higher number of posts on Twitter than on Facebook). However, it is also plausible, although not conclusively stated, that this data is supported by the general engagement of users being higher on Facebook than on Twitter, indicating a more loyal following on the former platform. This second conclusive hypothesis is further supported by the fact that Facebook has achieved a higher number of reactions and likes, as mentioned in the previous paragraph.

It's worth noting that the Instagram account was created in 2023, so it's logical that it has fewer followers, and the loyalty of these followers may be lower than on other platforms. However, despite having only 114 followers, it has generated 2.1k impressions and obtained a number of reactions and likes that is not significantly different from the achievements on other platforms—only 2.4 times less than Facebook and 1.52 times less than Twitter. Instagram has managed to gather 336 reactions compared to the 512 on Twitter and 804 on Facebook.



Figure 3. Comparing numbers and social media channels

Analysing the type of content that has performed best on social media during the ECSM 2023 campaign, photographs or illustrations are the format with the best functioning.

- The type of content that has been seen by the largest number of people (with a reach of 57k) and has generated the most interest, obtaining 755 clicks, has been photos or illustrations.
- The second most engaging content (with a total of 152 clicks) has been albums, despite being seen by five times fewer users than videos (albums had a reach of 6.4k, while videos had a reach of 32k).
- The third most engaging content has been videos. It's noteworthy here that despite having a 32% reach, they only obtained 12% of the clicks.
- The type of content that generated the least interest, with the lowest reach and the fewest clicks, has been links.

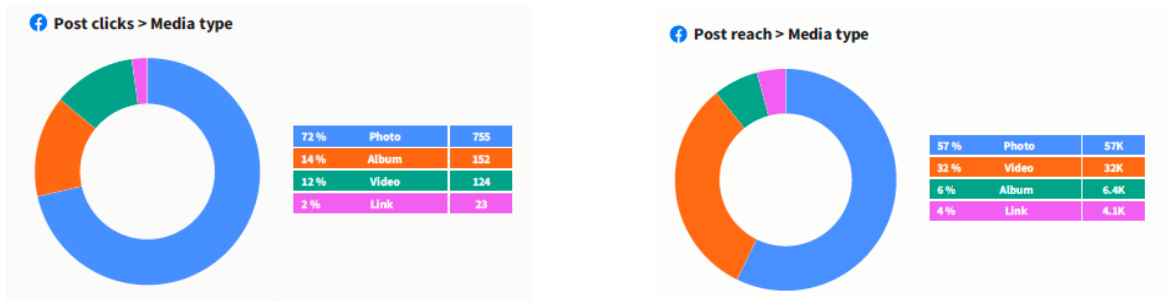


Figure 4. Clicks and reach sorted by media type

If we examine **which specific posts have generated the most interest**, the following observations emerge:

On **Facebook**, the post that has elicited the highest number of reactions is the **kick-off for the Cybersecurity Awareness Month**, followed by posts published on specific days related to cybersecurity—particularly, **Systems Administrators Day and World Password Day**. On these days, specific content was shared to commemorate these occasions.



Illustration 12. Top 3 posts on Facebook

Following this ranking of the top three highlighted posts on Facebook, the subsequent posts are listed in descending order based on the general interest they have generated on the mentioned platform.



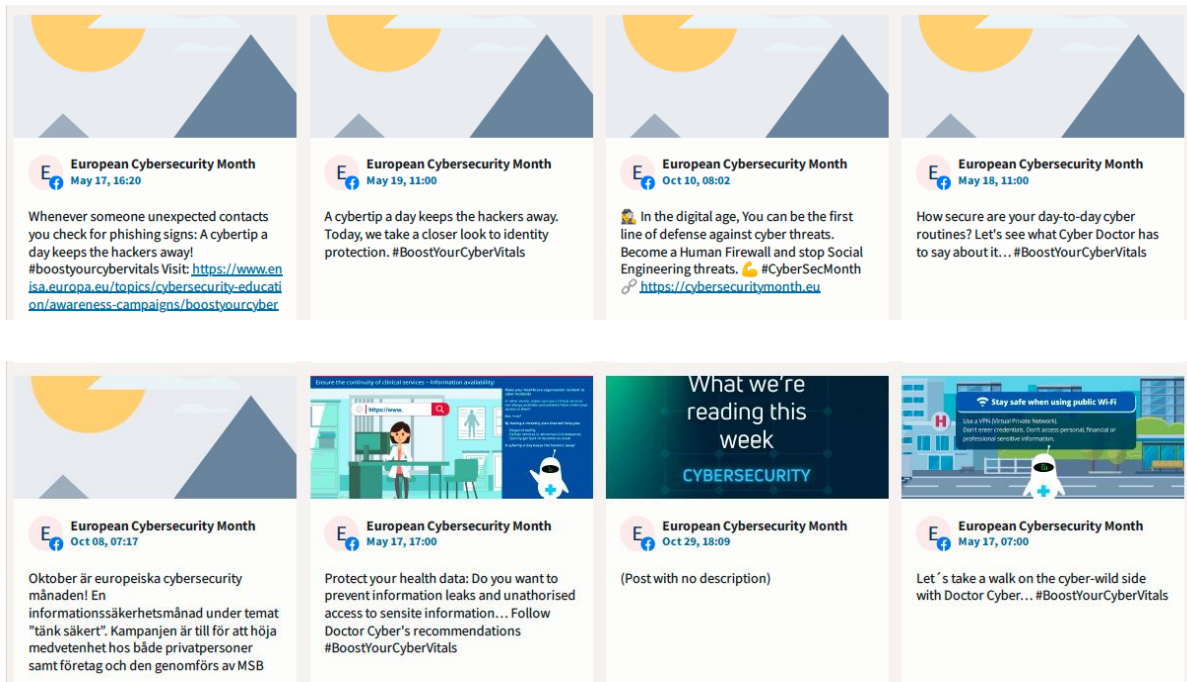


Illustration 13. Top 12 posts on Facebook

On **Twitter**, we observe that the tweet generating the most interaction or interest (engagement) is the one dedicated to downloading the **October campaign poster under our umbrella concept "Be Smarter Than a Hacker"**. The second most engaging tweet is the one precisely created for the **Annual Awareness Raising Awards ceremony celebrating Slovenia's video victory**. The third post that has harvested significant interest is the one referring to **Switzerland's adaptation of the Be Smarter Than a Hacker song**, produced specifically for this campaign.

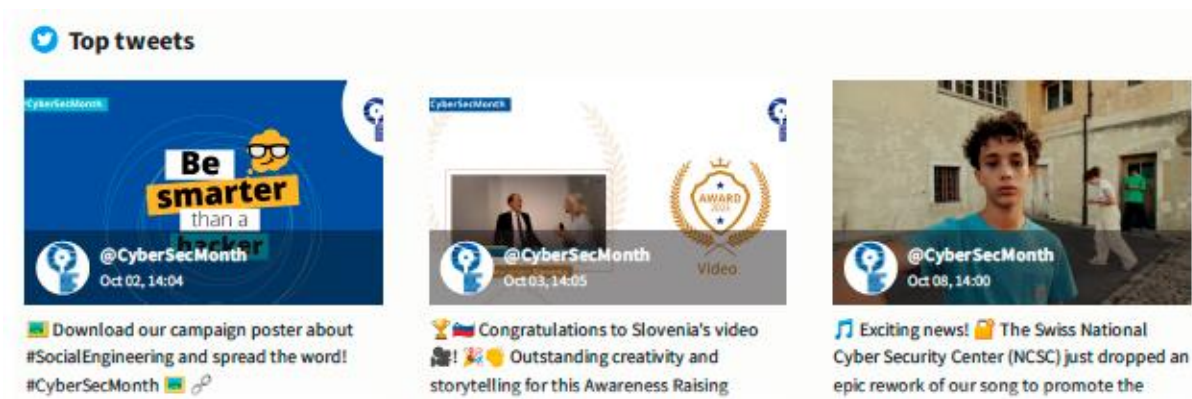


Illustration 14. Top 3 posts on Twitter

Following this top three of tweets, the subsequent tweets are arranged from highest to lowest based on the general interest they have generated on the platform.

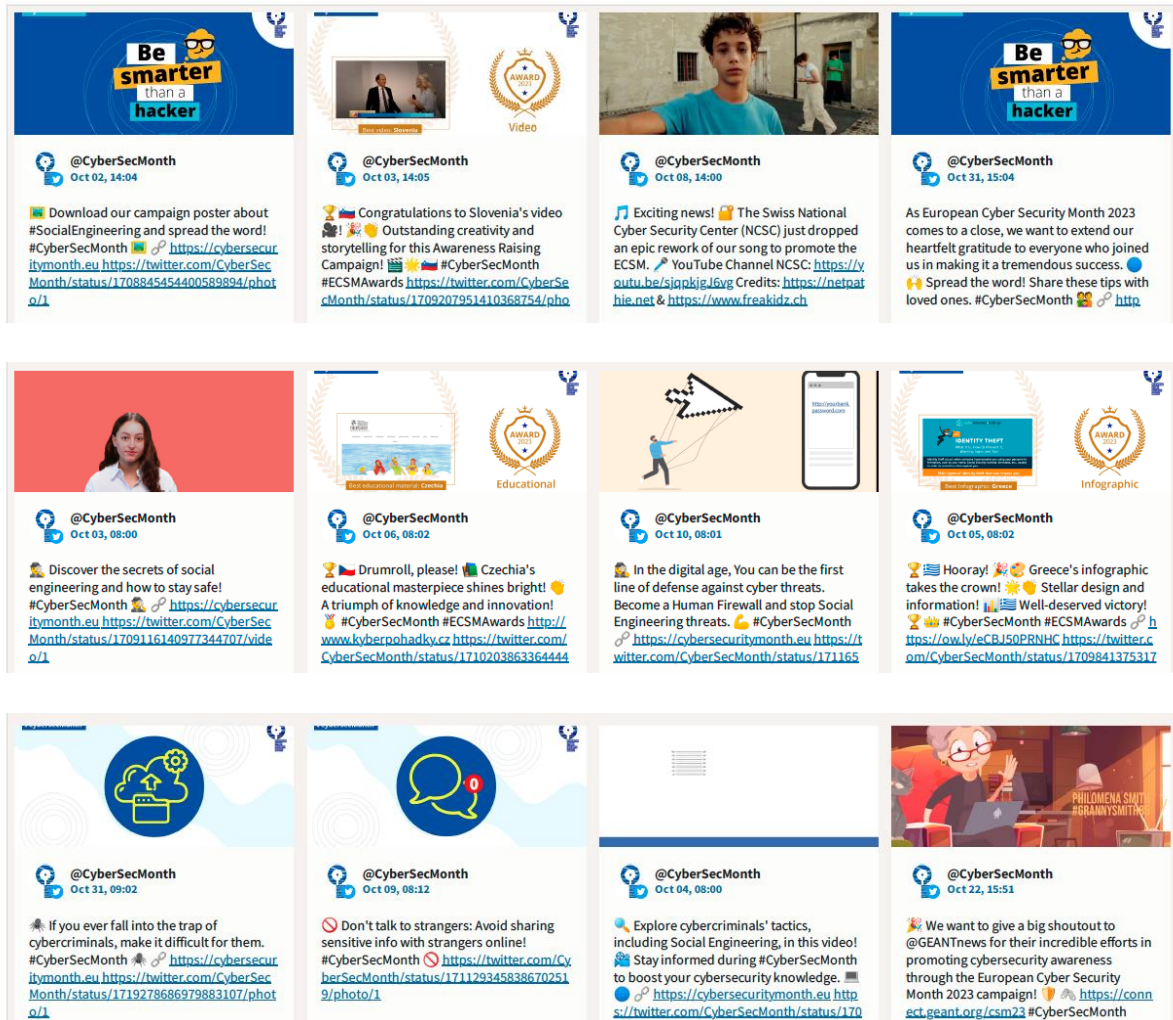


Illustration 15. Top 12 posts on Twitter

On Instagram, the posts that have performed best are also related to the **Be Smarter Than a Hacker** song. The adaptation from Switzerland has generated the most interest, followed by the English version of the song created for the campaign (from which the adaptation stems). The third post that has sparked considerable interest is the one about **unexpected request to protect yourself from social engineering attacks**.

In contrast to the analysis conducted earlier, on Instagram, we observe that the type of content that works best for this platform and audience is videos.



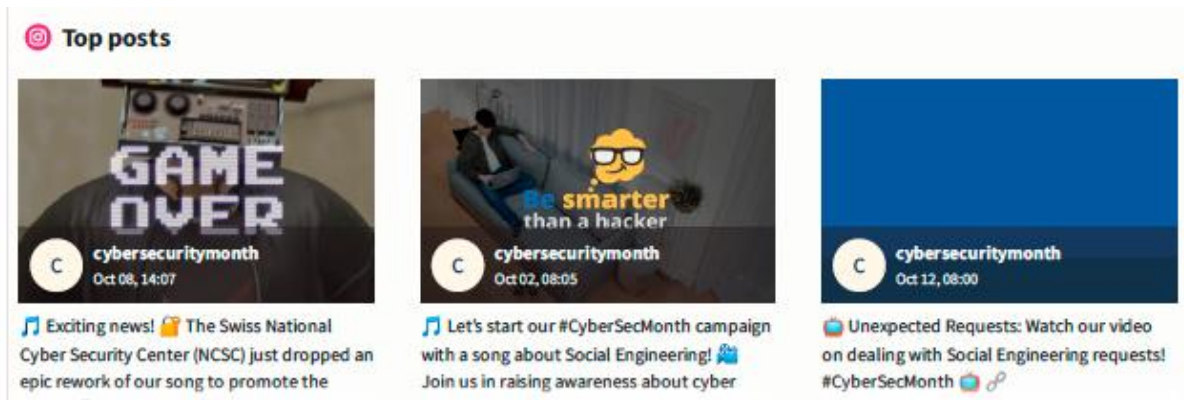


Illustration 16. Top 3 posts on Instagram

After this top three of posts on Instagram, the subsequent posts are also ordered from highest to lowest based on the general interest they have generated on the platform.

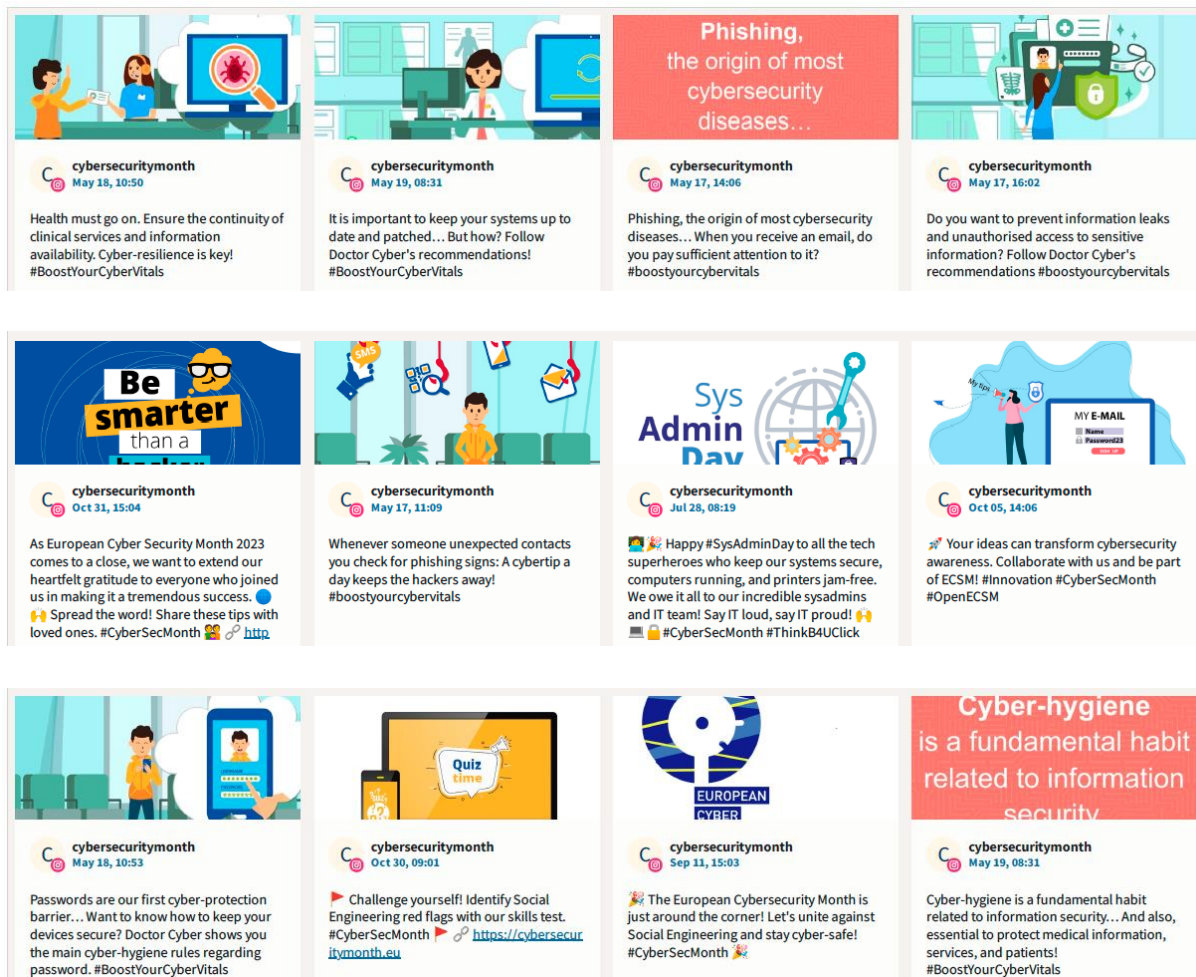


Illustration 17. Top 12 posts on Instagram

Having analysed the statistics based on the published posts, it is now crucial to study and understand how this year-long campaign has impacted ENISA's social media presence. This is examined by assessing the number of followers on each platform and how these numbers have either grown or decrease throughout 2023.

The total count of followers across all social media platforms directly and proactively utilised by ENISA during the ECSM 2023 campaign is 34k users. This marks an increase compared to the previous year, **with a gain of 481 new followers.**

The distribution of these followers is uneven. As observed in the earlier analysis, the @CyberSecMonth Twitter account boasts a total of 32k followers, while on Facebook, there are 1.9k followers (almost 17 times fewer than on Twitter). Meanwhile, on Instagram, there are 114 followers (equating to 280 times fewer followers than on Twitter and nearly 17 times fewer than on Facebook).

ENISA's social media presence has been reinforced with an increase in followers during the ECSM 2023 campaign



Figure 5. Followers by social media channel

The followers on Facebook have been steadily increasing uniformly throughout the entire year until October, where the growth surges and becomes more noticeable.

This trend indicates that the decision to extend the campaign across the entire year has yielded positive outcomes in effectively boosting both the number of followers and their engagement with ENISA's cybersecurity awareness initiatives.

As previously mentioned, the uniformity in the dispersion of the follower growth curve is disrupted in October, aligning with the cybersecurity awareness month campaign. This lines up with the anticipated and desired outcome, as the number of actions increases during this month, signifying that the initiatives have proven to be effective.

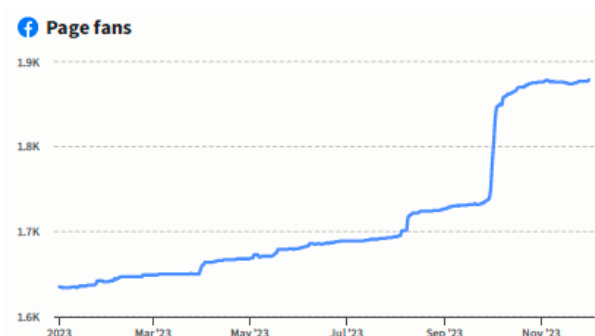


Figure 6. Facebook followers increase over time

If we examine the growth of followers on the **Instagram** account, which, as emphasised earlier, was created for the 2023 campaign, we observe that **all the increase occurs at the beginning of the cybersecurity month, October**. Once again, while the initial annual campaign goals may not have been fully achieved, there has been a noticeable rise in the number of followers with the commencement of the most significant campaign of the year in October.

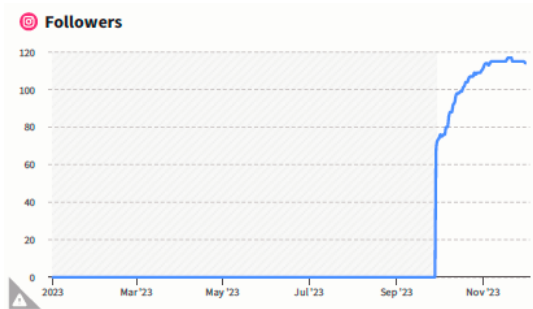


Figure 7. Instagram followers increase over time

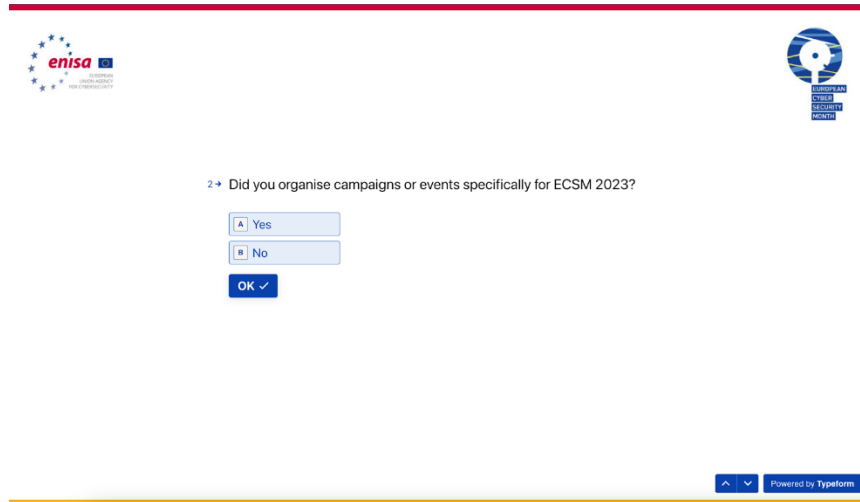
If we delve into the **demographic distribution**, considering the age characteristics of the followers, we can draw the conclusion that **we are effectively reaching the target audience for this campaign—the general public**.

Page fans > Age	
35-44	602
25-34	437
45-54	394
55-64	226
65+	132
18-24	82
13-17	4

Figure 8. Impacted audience sorted by age

4.2 ENGAGING MEMBER STATES

To measure both the level of engagement and satisfaction of Member States with the ECSM created, designed and produced by ENISA, the following survey was conducted:



2 → Did you organise campaigns or events specifically for ECSM 2023?

Yes

No

OK ✓

Powered by Typeform

All respondents organised specific events for the ECSM 2023.

Illustration 18. EUSurvey

Only 8 of all MS involved in the ECSM 2023 campaign together with the Ministry of Economic Affairs and Climate Policy completed the questionnaire: Croatia, Cyprus, Estonia, Greece, Italy, Poland, Slovenia, Sweden. Therefore, even though the conclusions are not representative of the entire campaign, we will rely on these numbers to extract results and lessons learned.

All of them organised specific events for the ECSM 2023, exceeding the ratio from 2022.

The **number of human resources** allocated for the organisation and launching of the ECSM 2023 **has ranged between 2 and 6 people**, being MS 5 the country that has designated the most assets in terms of manpower. The specific departments that somehow participated in the process were **Awareness, IT Security and Communications**. **The number of human resources is much lower than in 2022.**

Considering that 4 (MS 7, MS 4, MS 6 and MS 8) out of the 9 responding MS did not spend any economic resources in this year's campaign, **the average budget invested in the ECSM activities was approximately 36.100€** (in comparison with the 483.118€ spent in 2022).

Sorting the MS from the ones with more expenditures to the ones with less, we find that **MS 1 was the country that designated and spent more budget** (with 144.378€), in the ECSM 2023 activities, followed by MS 2 (with 96.000€), MS 3 (with 38.320€), MS 5 (with 30.000€) and MS 9 (with 5.000€). If we calculate the average budget contribution considering only the countries which indeed allocated economic resources, the amount rises to 56.700€.

The majority of respondent countries, 7 out of 9, used the materials created by ENISA for this 2023 ECSM campaign. Nevertheless, this figure must be taken with caution, as MS 1 and the MS 6 answered in one of the survey's questions that they did not use ENISA's content but specified the contrary in other answers. It is fair to conclude that **all MS who completed the survey did use in one way or another the content created by ENISA.**

Of the resources created by ENISA for the ECSM 2023 campaign, **the most widely used by MS have been videos and social media posts**, which according to the MS who filled the

All respondents employed the content created by ENISA in their own ECSM campaigns.

survey have been **utilised by all countries except MS 5, which has chosen** not to use these materials directly but **to adapt their content to their own population**. On the other hand, albeit to a lesser extent, respondent countries have also made use of the landing page specially created for this purpose, newsletters, paid media, and others, such as printed content, radio and TV media, infographics, etc. Only 2 of the MS have followed the Campaign Management.

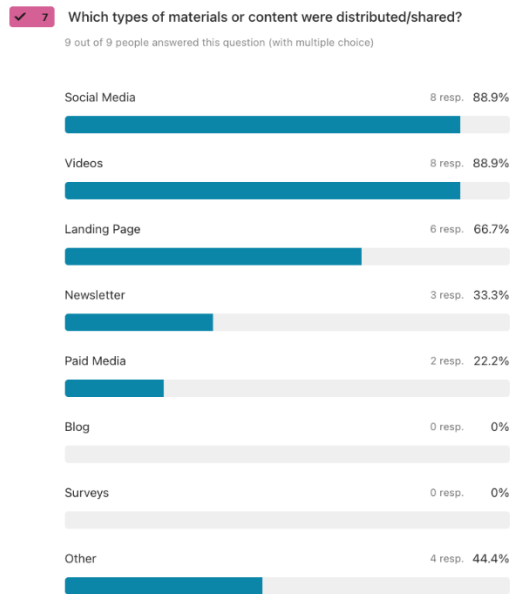


Illustration 19. Types of materials distributed by MS

Apart from MS 1, all answerers indicated that the ECSM created by ENISA added value to their own national campaigns. Both in the public (stated by all MS except from MS 2, that has particularly referred to industrial associations) and the private sector (also specified by all countries, with the exception of MS 3 and MS 8).

Excluding MS 1, all repliers indicated that ENISA successfully managed to share and promote innovative and creative content for the ECSM 2023. Obtaining an average evaluation score of 7 out of 10 (slightly higher than the feedback received from the 2022 campaign). In general terms, the subjective evaluation of the campaign by the involved MS is better than last year.

8 out of 9 MS indicated that ENISA has successfully added value to their national campaigns and has created and share innovative and creative content, with ENISA's work and efforts being evaluated at 7 out of 10.

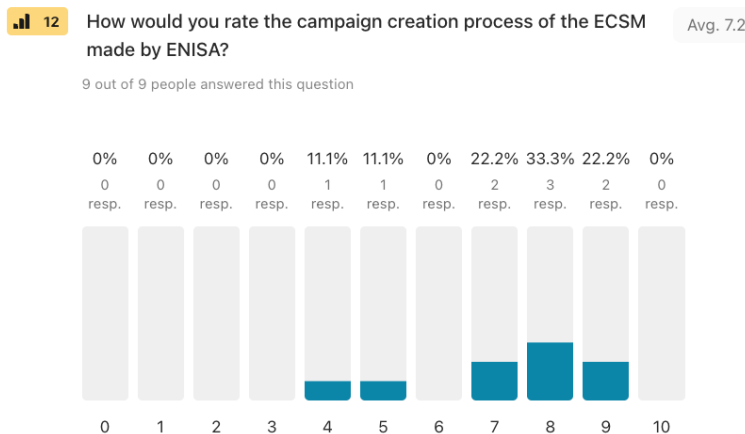


Illustration 20. Rates for the campaign given by MS

Analysing the **Key Performance Indicators (KPIs)** gathered to measure the success rate of the ECMS 2023, the following results are extracted:

- **Only 4 out of 9 MS allocated economic resources to online media.**
- Comparing the unique visitors to the landing page resulting from the 2023 campaign to the 2022 campaign, the following highlights should be noted - **all responding MS achieved an increase in unique visitors.** The most significant increase was perceived by MS 2 as all of their visitors were new, given that they did not receive any visitors in 2022. This increase is followed by MS 3, whose visitors count surged by 89%. MS 4 experienced a 40% increase over the 2022 numbers, and MS 7 a 23% raise. Although the metrics for MS 1 and MS 8 are incomplete and cannot be compared to any 2022 figures, they received 14.247 and 1.487 unique visitors, respectively.
- Studying the landing page time interaction in October 2023 compared to the same period in 2022, the following conclusions can be drawn. The only two countries whose metrics can be compared are MS 3 and MS 8. In both cases, **the average time interaction has increased compared to the numbers obtained in 2022.** Visitors spent 35 seconds more on MS 3's landing page, and 11 seconds more on MS 8's. Again, we do not have enough information to compare the results in the cases of MS 2 and MS 1, but we do know that visitors spent an average of 4 minutes and 29 seconds on the first's, and 1 minute and 37 seconds on the second's.
- **The most utilised social media channels were Facebook, Instagram and LinkedIn.** All of which were employed by 77,78% of the MS that replied to the survey. Even though to a lesser extent, YouTube was also used, this time by 44,44% of the respondents. The social network that was not implemented during the ECSM 2023 was TikTok.

Both unique visitors and the time spent on the website increased in all MS particular cases compared to the statistics from the year 2022.

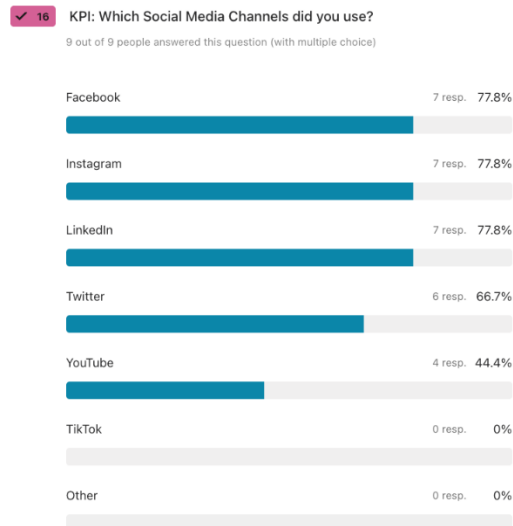


Illustration 21. Social media channels employed by MS

- Analysing the engagement achieved on social media by the answerers, some notable elements emerge. In all cases with sufficient data for analysis, **it is consistently observed that the reach exceeds engagement, which is expected.** The countries, ranked from the highest to the lowest engagement, are MS 2 (with 10.008), MS 8 (with 4.852), MS 3 (with 3.904), MS 4 (with 2.384) and MS 7 (with 398).
 Having only five cases in which the data can be directly compared, **one of the lessons learned arises:** to minimise variation in the types of collected data and address this matter for

future campaigns, **the process should be homogenised and standardised**, collecting the same type of entries for all countries.

- With regard to the engagement achieved through the utilisation of **YouTube** during the ECSM 2023, the following observations are made. Once again, ranking the responding MS from the most **views** achieved to the least, **MS 5 stands out with almost 3 million views**, followed by MS 1 with 97.675, MS 2 with 2.218, MS 3 with 1.699, MS 7 with 1 and MS 4 with 0.
- **Only 4 out of 9 of the responding MS made use of the hashtag Be Smarter Than a Hacker. This outcome was expected**, as a debate ensued when it was proposed due to the use it makes of the word “hacker” understood as a cybercriminal. The conclusion of the discussion was for MS who were in favour of using it, to indeed implement it in their publications, and for those who were not in favour, to apply other hashtags such as #ThinkBe4Uclick.
- Following an initiative created for the ECSM 2023 campaign, a new hashtag was also proposed: #OpenECSM. **The Open ECSM was a sub-campaign initiative** that encourage individuals to actively participate in the ECSM by sharing their own experiences and insights related to the topic of the 2022 campaign on their personal social media channels, further explained below in the present report. **#OpenECSM was employed by 5 out of the 9 respondents.**

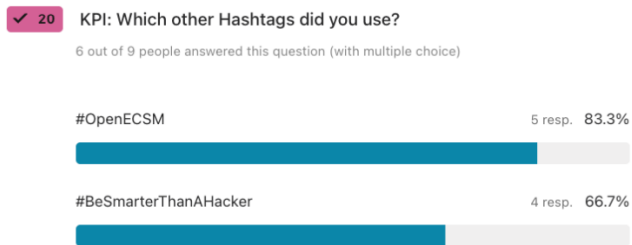


Illustration 22. Hashtags employed by MS

5. CONCLUSIONS & RECOMMENDATIONS

For the ECSM 2023 campaign, four **innovations** were introduced and worked on.

Firstly, it is the first time that **the cybersecurity month is decided to be celebrated throughout the entire year**. This idea was born for the purpose of enhancing the reach of cybersecurity awareness, aiming to increase the perceived importance of this knowledge area among users.

Secondly, **it is the first time that a song was created as the main content** of the ECSM campaign. The song as a creative content has been well-received by all MS, leading some of them to even create their own versions.

Thirdly, there was **an effort to include all the people who work behind the scenes and make it possible for the ECSM campaigns to be carried out** and have been running for all these years. This proposal has been called OpenECSM.

Lastly, it is **the first time that ENISA worked with the social media platform Instagram**. Since the ECSM 2023 campaign targeted the general public, it was necessary to also start working with this social media platform.

The ideas and creations for the ECSM 2023 were highly welcome by both Member States and the targeted audience. This resulted on a better evaluation of the whole campaign, receiving better feedback than past campaigns, despite the fact that paid social media could not be employed and the campaign only relied on organic posts.

Having the aforementioned in mind and **analysing ENISA's presence growth on social media**, the following points are also noteworthy:

- **The number of followers increased on all platforms.**
- **Twitter is the platform where ENISA had the highest number of followers.** Despite sharing on it the least content, it has generated the most impressions.
- The number of reactions on Twitter and Facebook is not significantly different, despite Twitter having a much larger follower count. This indicates that **Facebook is the social media platform where ENISA has the most loyal audience.**

In relation to **MS feedback**, the following points are also worth highlighting:

- **All MS that completed the survey have directly used or adapted the deliverables created and produced by ENISA** for the ECSM 2023.
- **Almost 90% of respondent countries have considered ENISA's efforts a success**, both in adding value to their own national campaigns and in creating content.
- During this campaign, **all responding MS have achieved growth in unique visitors and the time these users spend on their websites.**

As **lessons learned**, it is clear that the survey format should be reanalysed to further narrow down response options. This would ensure that responses from all MS are more standardised and homogeneous, allowing for better comparisons and more representative conclusions.



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 978-92-9204-665-1

DOI 10.2824/005990