



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ



Press Release

European Cybersecurity Month 2022: Ten Years of Raising Cyber Awareness Throughout Europe

Bucharest, September 30, 2022

The 10th edition of the European Cybersecurity Month (ECSM), an event that promotes online security among European users, begins today. The Romanian National Cyber Security Directorate (NCSO) is part of the ECSM since its pilot project in 2012 and acted as a national coordinator and member of the organising team at EU level.

Today, the [European Union Agency for Cybersecurity](#) (ENISA) starts, together with EU Member States, the activities of the ECSM awareness campaign. This year's European Cyber Security Month was officially launched by **Margaritis Schinas**, European Commission vice-president for promoting our European way of life. Watch the video [here](#).

For its 10-year anniversary, the 2022 edition of the ECSM will be focusing on **PHISHING** and **RANSOMWARE**, with a series of activities taking place all over the EU throughout October.

Conferences, workshops, training sessions, webinars and quizzes are some of the many activities organised by ENISA and the Member States. The [campaign activities](#) users can participate in are available on the [ECSM website](#). In order to better promote Member State campaign materials and showcase stakeholders' activities, ENISA added this year the "ECSM Awards" initiative for the most successful awareness materials to the campaign.

Ultimately, the goal of the ECSM campaign is to strengthen the resilience of EU systems and services by enabling citizens to act as effective human firewalls and thus take a step further towards a more cybersecurity-smart society.

The 2022 edition of the ECSM aims to reach professionals between 40-60 years of age from all sectors of the economy, focusing especially on SMEs. It is also intended for the European business community as a whole and for people whose work depends on digital technologies and tools.

The 2022 European Cybersecurity Month (ECSM) coincides with its 10-year anniversary, since a pilot was first launched in 2012. The campaign is now an integral part of the actions designed to implement the provisions of the [EU Cybersecurity Act](#) on awareness raising and education.

"In recent years, attacks on European users have become increasingly frequent and complex. Unfortunately, cybercriminals often manage to compromise, with minimal investment, computer systems, websites or devices. Cybersecurity is a shared responsibility, so it is necessary that each of us regularly update our daily security routine and hygiene to keep up with these threats. The European Cyber Security Month offers a series of extremely useful tools for the common user, through which he can attain vital security reflexes when active in the online environment," said **Dan Cîmpean**, the NCSO Director.

Margrethe Vestager, European Commission executive vice-president for a Europe fit for the digital age, said: "Some of the biggest risks to our IT systems and networks can occur through human error. Learning to stay cybersecure is a daily task for all of us, and the European Cybersecurity Month will help us step up to it."

Margaritis Schinas, European Commission vice-president for promoting our European way of life, stated: "The European Cybersecurity Month is a flagship activity, part of our efforts to help EU citizens

and stakeholders to be safe online. While shielding the EU with a panoply of actions to protect its security. We need informed citizens who are part of our Security Union. This year's campaign will help everyone learn and understand how to protect their daily life from new emerging threats such as ransomware."

Thierry Breton, European commissioner for the internal market, declared: "As our societies become increasingly interconnected, the cyber risk is expanding. One of the best ways to protect ourselves is through training and cyber literacy, including in everyday life. That's what the Cybersecurity Month is all about, and it has well proven its worth over the past 10 years."

Juhan Lepassaar, ENISA Executive Director, added: "The number of successful online attacks could be greatly reduced if more people knew how to detect and react. This is what the activities of the European Cybersecurity Month are all about. The new awards introduced this year will give more visibility and incentive to develop tools and campaigns to help EU citizens. It marks a further step in the ten-year development of the ECSM. Building a trusted and cyber secure Europe also means to help all businesses thrive in a secure digital environment."

The ECSM Awards

The ECSM Awards is a new initiative falling into the activities of the ECSM campaign. Here, Member State representatives involved in the process will vote every year for the most innovative and impressive materials produced for past ECSM campaigns. Members States were asked to vote from a list of campaign material submitted to the competition.

Congratulations to the winning EU Member States for their successful materials!

- **Best Infographic:** Ireland - [Become your own cyber security investigator](#)
- **Best Teaching Material:** Greece - [Treasure hunt games for primary school](#)
- **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](#)

For the 2022 awards, the winning material will be translated in all EU languages and will be promoted anew within the running year's campaign. ENISA aims to organise this competition every year.

Phishing & Ransomware in brief

Phishing is a type of attack performed in a digital communication. The targeted victim is lured into providing personal information, financial data or access codes by an attacker pretending to be trustworthy. The only way to counter these attacks is to empower people and give them the right tools and tricks to detect them and avoid falling into the traps.

Ransomware has been identified as the most devastating type of cybersecurity attack over the last decade, impacting organisations of all sizes around the globe. It is another type of digital attack, which allows threat actors to take control of the target's assets and demand a ransom in exchange for the availability and confidentiality of these assets.

Press contact person: Mihai Rotariu | mihai.rotariu@dnsc.ro | 0740 066 866