enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

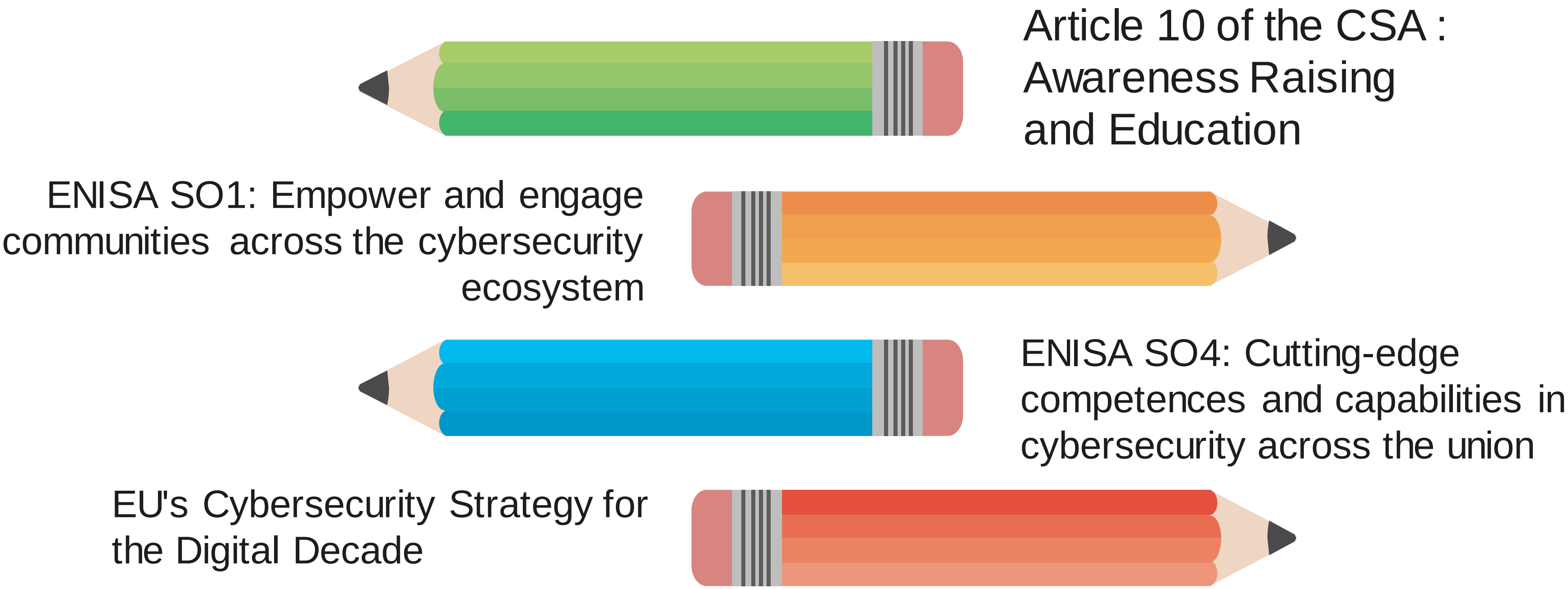
BUILDING CYBERSECURITY AWARENESS

The ENISA Awareness Raising Framework

Georgia Bafoutsou
Awareness Raising and Education Team
ENISA- European Union Agency for Cybersecurity

11 | 05 | 2022 - 1st NISDUC Conference, Luxembourg

BACKSTAGE



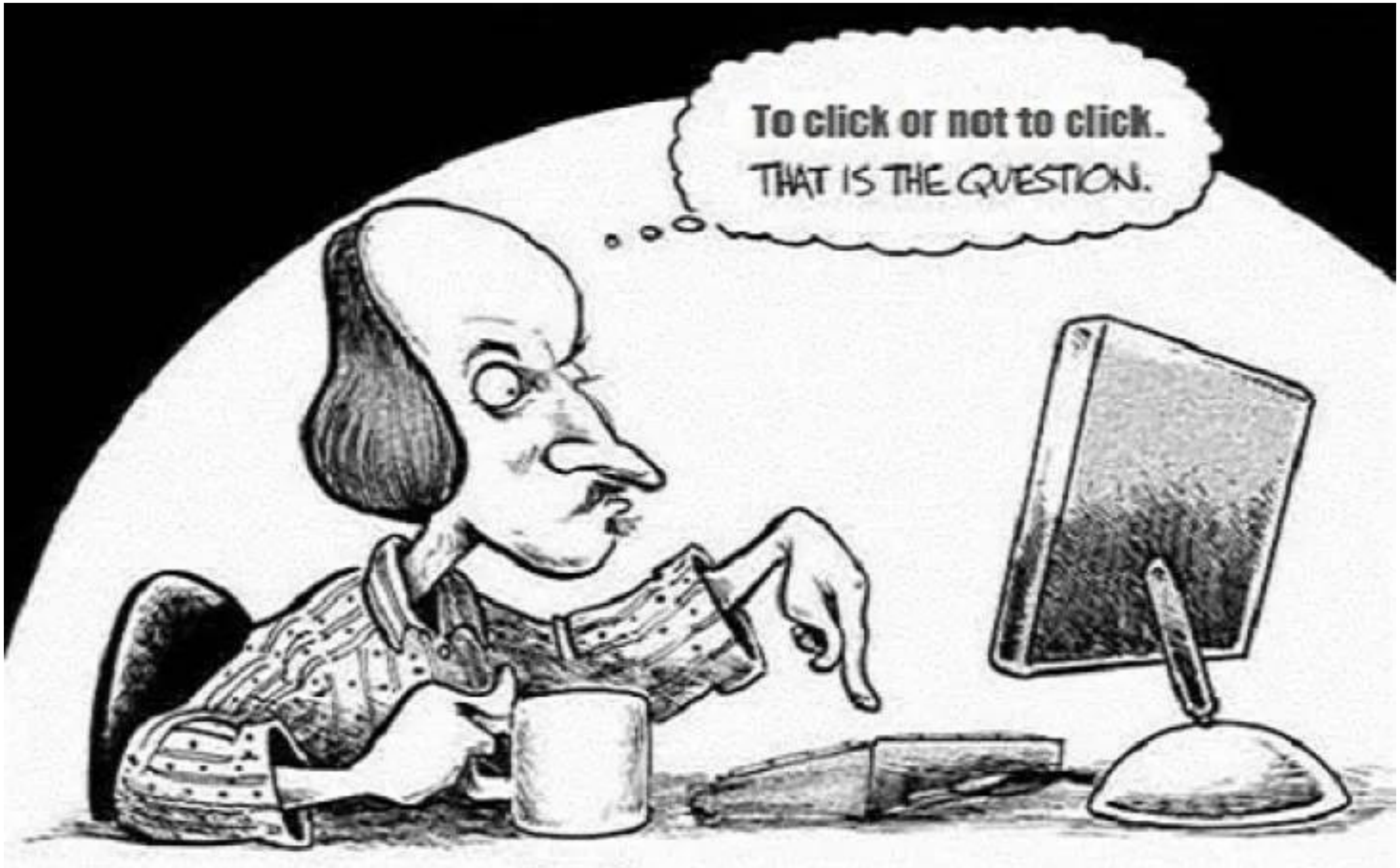
Article 10 of the CSA : Awareness Raising and Education

ENISA SO1: Empower and engage communities across the cybersecurity ecosystem

ENISA SO4: Cutting-edge competences and capabilities in cybersecurity across the union

EU's Cybersecurity Strategy for the Digital Decade

VISION



To achieve mind-set and behavioural change towards cybersecurity

MISSION

AWARENESS

Increase citizens', organisations' and businesses' awareness of cybersecurity.

PROMOTION

Promote cybersecurity best practices and solutions to citizens, organizations and businesses.

DISSEMINATION

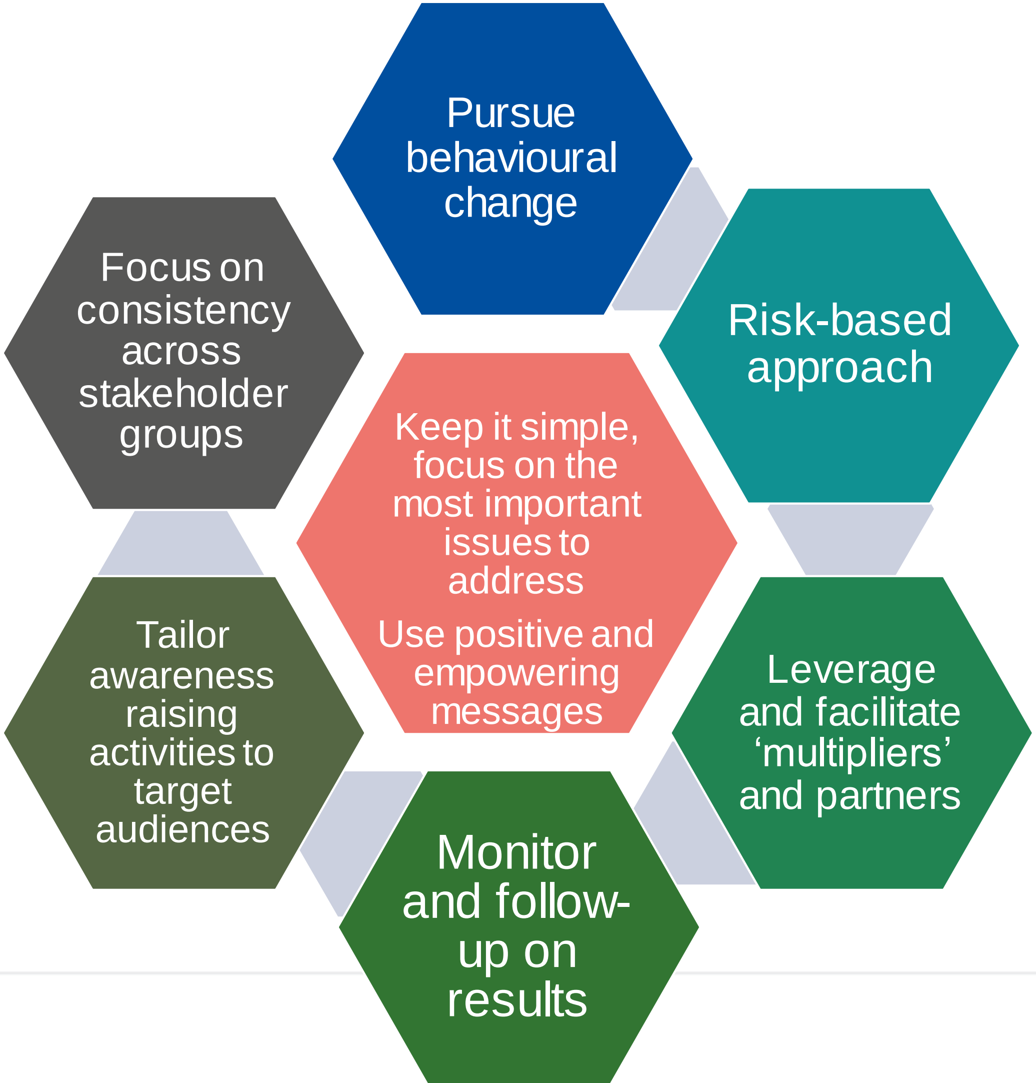
Provide consumers with information on applicable certification schemes and cybersec level of ICT products, services and processes.

EDUCATION

Organise joint education campaigns directed at end users and support cyber skills development in the EU

AWARENESS RAISING FRAMEWORK

GUIDING PRINCIPLES



Pursue behavioural change

Risk-based approach

Leverage and facilitate ‘multipliers’ and partners

Monitor and follow-up on results

Tailor awareness raising activities to target audiences

Focus on consistency across stakeholder groups

Keep it simple, focus on the most important issues to address

Use positive and empowering messages

ARET CAMPAIGNS 2021-2022

EUROPEAN CYBERSECURITY MONTH

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

- Annual Campaign
- Promote cybersecurity
- Provide up-to-date online security information through awareness raising and sharing of good practices

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

European Commission

HIGHLIGHTS ECSM 2021

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

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

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

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

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

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

DIVERSITY IN CYBERSECURITY

CYBERSECURITY: A FASCINATING CAREER PATH

Did you know that only 7% of cybersecurity experts in the EU are women?

BE PART OF OUR COMMUNITY

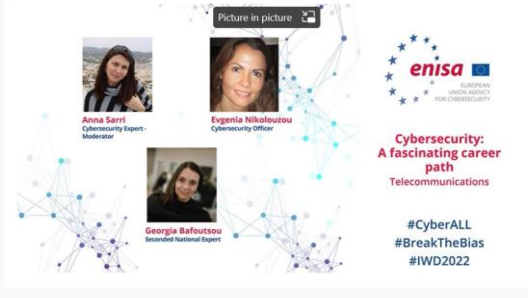
https://enisa.europa.eu

#CyberALL #IWD2022

The ECSC provided an opportunity to network with industries and universities, but also to improve technical skills. There are already many girls in the competition, and we are definitely bringing our own touch. If you like cybersecurity, you should not compare yourself to boys. Just forget about the stereotypes, break the boundaries and just jump into it!

SOPHIA AND KATY, UK

#women4cyber



Anna Sarri
Cybersecurity Expert - Moderator

Evgenia Nikolouzou
Cybersecurity Officer

Georgia Bafoutsou
Seconded National Expert

Cybersecurity: A fascinating career path
Telecommunications

#CyberALL
#BreakTheBias
#IWD2022

#WOMEN4CYBER
#CYBERALL

During 2021 we run Women4Cyber and in 2022 CyberAll campaigns

- Showcase the presence of women in Cybersecurity
- Close the gender gap in the technological field
- Also highlight the importance of diversity

Resources: Social Media, Online panels, EC Women for Cyber Registry, Podcasts

https://www.youtube.com/watch?v=vuUNpa2pONk

https://www.youtube.com/watch?v=UlyD4PbKuiM

https://www.youtube.com/watch?v=-UmZz8LQu1o

DIVERSITY IN CYBERSECURITY

#CYBERALL

CYBER-GIRLS

Meet the girls behind the European Cybersecurity Challenge to discuss women's future in cybersecurity

Virtual Event - 10 March

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
EUROPEAN CYBER SECURITY CHALLENGE

2022 initiatives:

In March 2022

- ➢ Hands-on training on binary exploitation for female Team EU candidates.

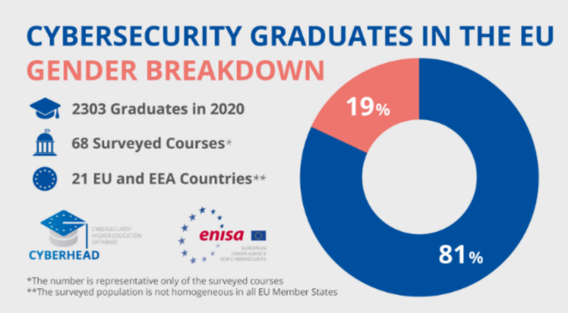
In September 2022

- ➢ Back-to-back event with ECSC 2022

Facts and Figures:

- ➢ ECSC 2019 only 8 female were members of the national teams
- ➢ ECSC 2021 - some MS have included gender balance as a prerequisite for the national teams for ECSC.
- ➢ ECSC 2022 - 15 girls (55 candidates) in Team EU

- ➢ **Stats from ENISA Cyber Higher Education Database (CyberHEAD):**



CYBERSECURITY GRADUATES IN THE EU

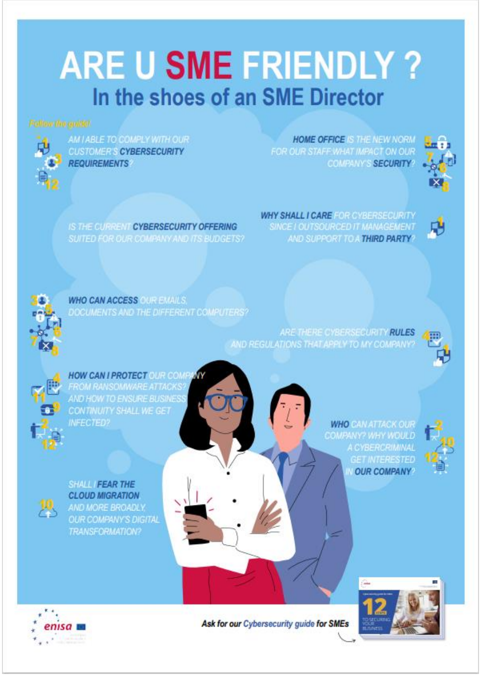
GENDER BREAKDOWN

*The number is representative only of the surveyed courses

**The surveyed population is not homogeneous in all EU Member States

CYBERSECURITY FOR SMES

“Are U SME friendly.”



ARE U SME FRIENDLY ?

In the shoes of an SME Director

Follow the guide!

AM I ABLE TO COMPLY WITH OUR CUSTOMER'S CYBERSECURITY REQUIREMENTS?

HOME OFFICE IS THE NEW NORM FOR OUR STAFF:WHAT IMPACT ON OUR COMPANY'S SECURITY?

IS THE CURRENT CYBERSECURITY OFFERING SUITED FOR OUR COMPANY AND ITS BUDGETS?

WHY SHALL I CARE FOR CYBERSECURITY SINCE I OUTSOURCED IT MANAGEMENT AND SUPPORT TO A THIRD PARTY?

WHO CAN ACCESS OUR EMAILS, DOCUMENTS AND THE DIFFERENT COMPUTERS?

ARE THERE CYBERSECURITY RULES AND REGULATIONS THAT APPLY TO MY COMPANY?

HOW CAN I PROTECT OUR COMPANY FROM RANSOMWARE ATTACKS? AND HOW TO ENSURE BUSINESS CONTINUITY SHALL WE GET INFECTED?

WHO CAN ATTACK OUR COMPANY? WHY WOULD A CYBERCRIMINAL GET INTERESTED IN OUR COMPANY?

SHALL I FEAR THE CLOUD MIGRATION AND MORE BROADLY, OUR COMPANY'S DIGITAL TRANSFORMATION?

Ask for our Cybersecurity guide for SMEs

- A study - Cybersecurity for SMEs: Challenges and Recommendations

https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

- Leaflet with 12 steps on how to secure your business.

https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

- SecureSME tool - that offers cyber tips and guidelines developed both from ENISA and from the National Authorities of the MS.

https://www.enisa.europa.eu/securesme#/

What’s next:

- **Focus on Ransomware and Phishing**
- **Support National Authorities**
- **Webinars** to multipliers and SMEs
- SME campaign **on tradeshows**
- **Adapt & reuse materials** (translation in all European languages)

CYBERSECURITY CERTIFICATION

"HAVE YOU HEARD ABOUT THE EU CYBERSECURITY CERTIFICATION SCHEMES?

EU
CYBERSECURITY CERTIFICATION
WHAT'S IN FOR CONFORMITY ASSESSMENT BODIES
BUT HOW CAN CAB GET READY?

Targeting the "ones that can certify": CABs, NCCAs

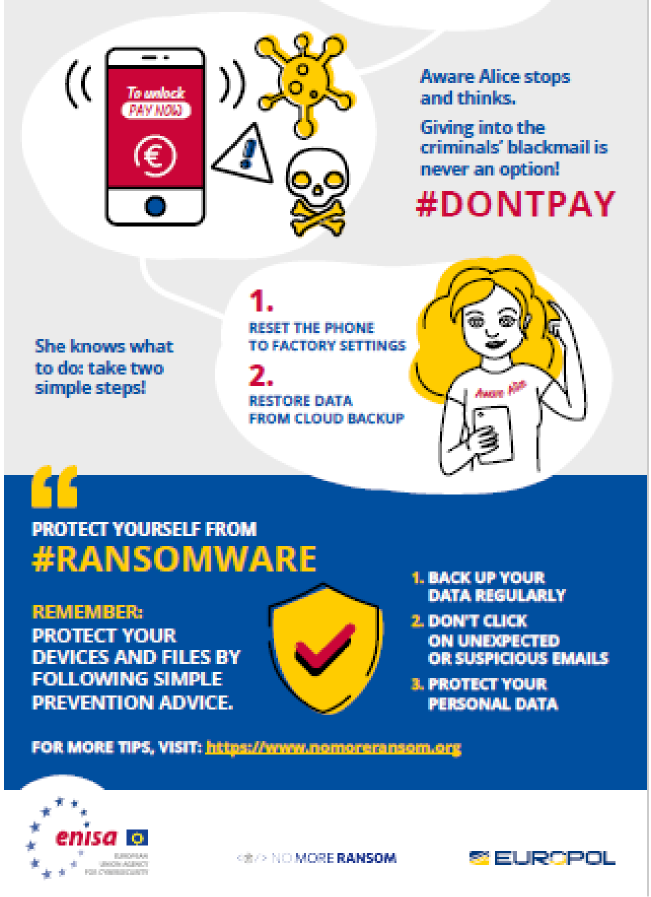
- ➢ bringing a good overall knowledge of how certification will work
- ➢ inviting them to seize the opportunity of EU certifications

How: Series of educational videos for different target audiences, Infographics, FAQ on website

2 campaigns :

- **In June** around the ENISA Cybersecurity Certification Conference: Create a **video** describing the **panorama of certification**, **organise workshop** with present stakeholders during the week
- **Late November-** many certification/Cybersecurity events around that time, Certification AHWG meetings – **publish a toolkit for main stakeholders** (NCCA, maybe CABs) , **supporting video**

#NOMORERANSOM WITH EUROPOL



Aware Alice stops and thinks.

Giving into the criminals' blackmail is never an option!

#DONTPAY

She knows what to do: take two simple steps!

1. RESET THE PHONE TO FACTORY SETTINGS

2. RESTORE DATA FROM CLOUD BACKUP

PROTECT YOURSELF FROM

#RANSOMWARE

REMEMBER:
PROTECT YOUR DEVICES AND FILES BY FOLLOWING SIMPLE PREVENTION ADVICE.

1. BACK UP YOUR DATA REGULARLY
2. DON'T CLICK ON UNEXPECTED OR SUSPICIOUS EMAILS
3. PROTECT YOUR PERSONAL DATA

FOR MORE TIPS, VISIT: https://www.nomoreransom.org

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY NO MORE RANSOM EUROPOL

Bring behavioural change on the topic of Ransomware

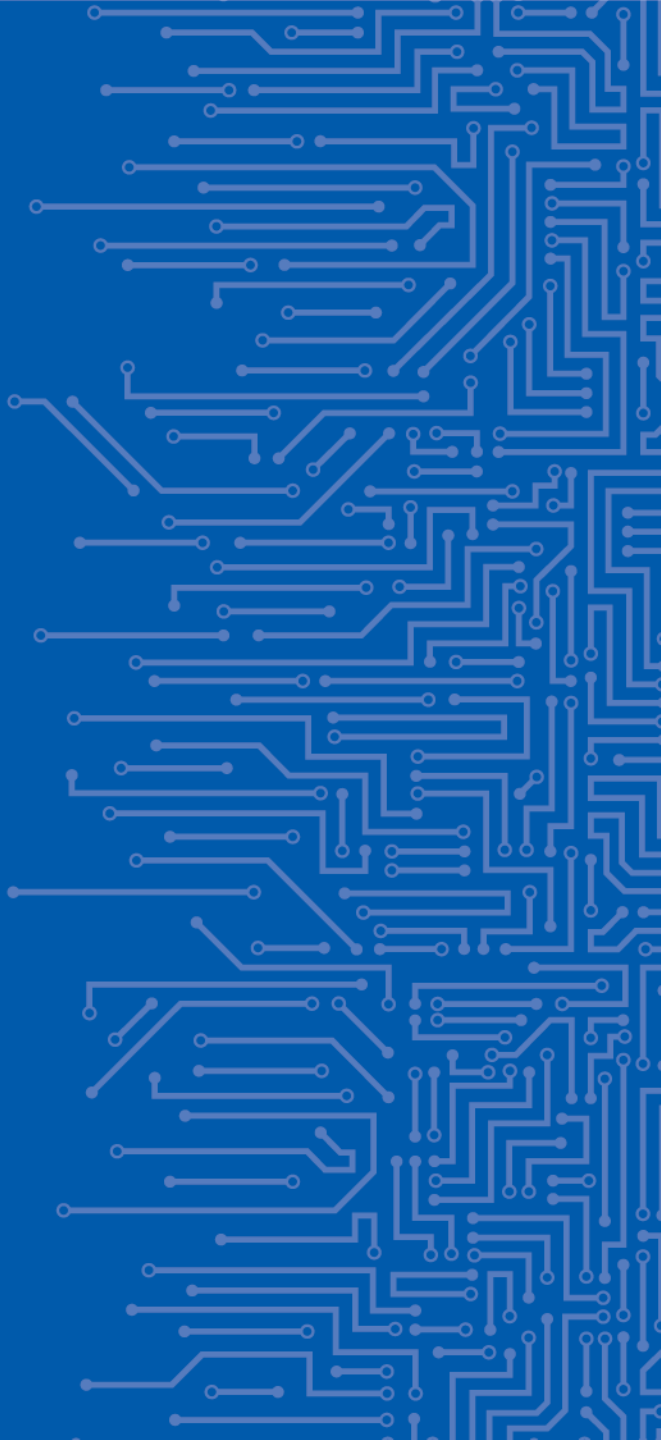
Campaign and Dialogues created in collaboration with Europol

Resources: infographics, video, social media dialogues

What's next:

- ➢ More campaigns on this topic (i.e. ECSM)
- ➢ Make recurrent co-campaigns with other EU institutions

NEW CAMPAIGNS – AR IN A BOX



2022 PLAN

- **Overall aim:**
  - Deliver activities targeting behavioral change to OES staff – with a focus to non-cybersecurity professionals
- **Planned deliverables:**

Awareness Raising campaign

Aim: Educate staff on how to avoid cybersecurity threats, minimizing incidents or reducing their impact

AR-in-a-Box

Aim: provide both theoretical and practical support, using a variety of awareness raising tools (e.g. videos, leaflets, exercises) offering AR as a service.

Practice

Aim: support the trainees/trainers to apply newly acquired knowledge on how to design and run AR campaigns

AR-IN-A-BOX: WHAT IS IT?

Framework for building awareness culture in an Organization

- Sector agnostic material
- Helps deal with real incident/ crisis via the right incident response steps

Communication Guide

AR Framework

Template Awareness Media

Awareness Table Top Game

AR-IN-A-BOX

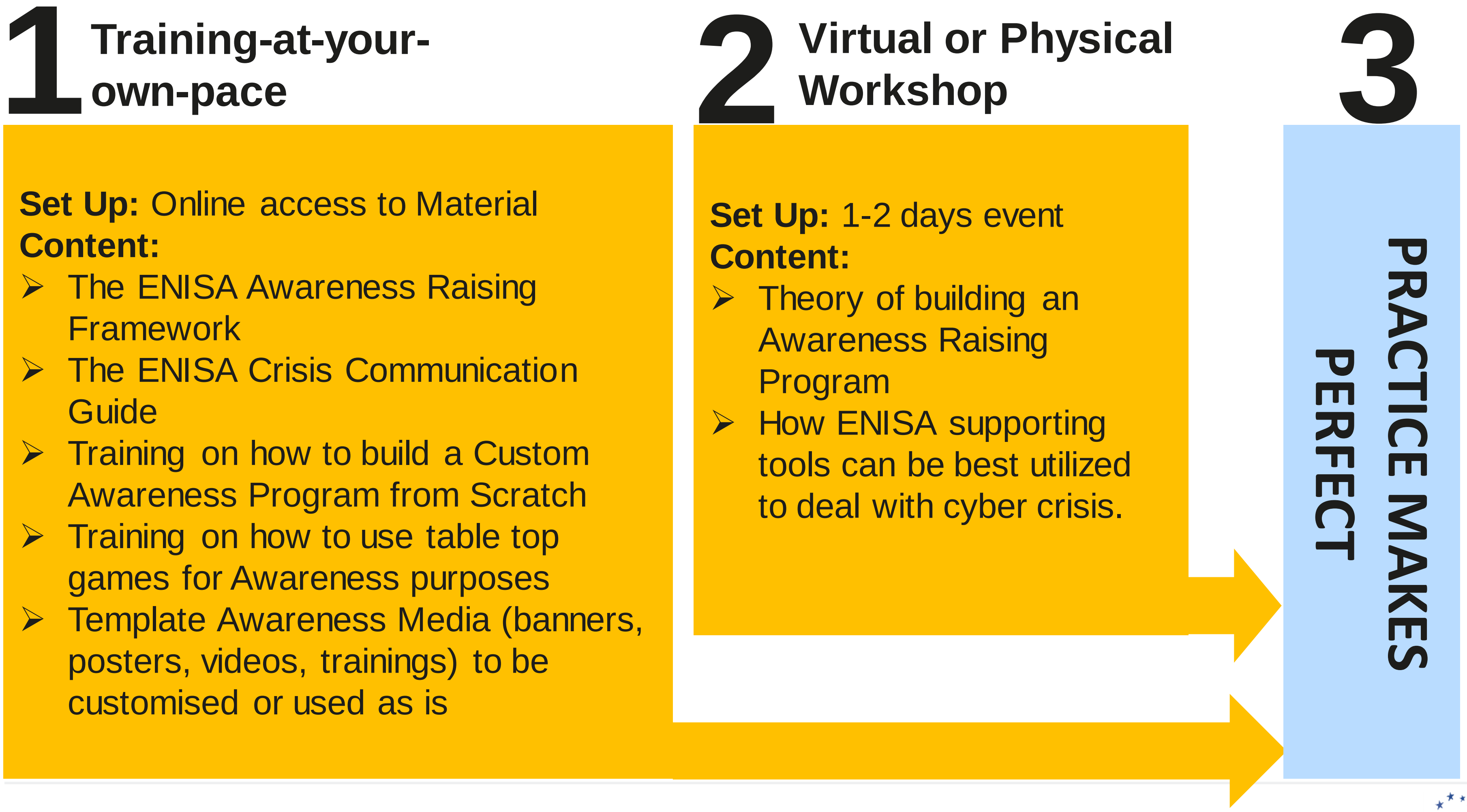
Practice on:

- ✓ How to build a Custom Awareness Program
- ✓ Communication basics
- ✓ How to use table-top games and regular quizzes for Awareness Raising

AR-IN-A-BOX: WHAT IT INCLUDES

- Steps to design, organize and execute an AR campaign
- Methodology to identify top human risks and the key behaviors that manage those risks
- Dissemination channels per target audience to create more impact
- Template material for i.e. communication strategy, playbook of activities, media templates (and recommendations on how to use them)
- Common practices for social media use
- Recommendations of KPIs and measurements and important tools
- Calendar for various activities including quizzes and game scenarios

AR-IN-A-BOX: METHODS OF DELIVERY



1 Training-at-your-own-pace

Set Up: Online access to Material

Content:

- ➢ The ENISA Awareness Raising Framework
- ➢ The ENISA Crisis Communication Guide
- ➢ Training on how to build a Custom Awareness Program from Scratch
- ➢ Training on how to use table top games for Awareness purposes
- ➢ Template Awareness Media (banners, posters, videos, trainings) to be customised or used as is

2 Virtual or Physical Workshop

Set Up: 1-2 days event

Content:

- ➢ Theory of building an Awareness Raising Program
- ➢ How ENISA supporting tools can be best utilized to deal with cyber crisis.

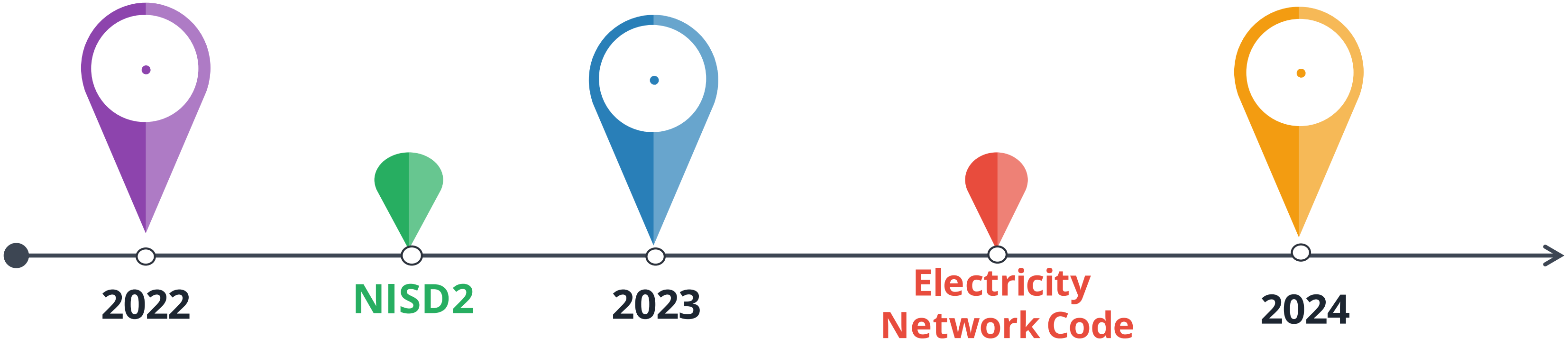
3

PRACTICE MAKES PERFECT

AR CAMPAIGNS ON OES

Year	Target sector	Notes
2022	Healthcare	- Low cybersecurity awareness and maturity - Prominent target for malicious actions- high number of medium impact incidents (as per Annual report NIS Directive Incidents 2020) - Low cybersecurity investment and skills in the Operators of Essential healthcare services Targeting the authorities due to the disperse nature of the sector
	Energy	- Highly interdependent sector - Awareness raising will be a legal requirement based on the CODE - Reported incidents under NISD show an increase of 200% in 2020 Targeting the OES directly
2023	Transport [2 modes]	- Low cybersecurity maturity - Raising awareness is in the portfolio of DG MOVE for the modes
2024	Water supply*	tbc
	Postal services*	tbc

3 YEARS AR PLAN: ENERGY



2022

NISD2

2023

Electricity Network Code

2024

Spike in Cybersecurity

Target audience: Energy Operators of Essential Services – DSO, TSO etc

Means: promotional material, AR in a Box train the trainer session of OES, e-learning, e-training, delivery of dedicated sessions for dissemination

Theme: Ransomware

Timeline: September 2022

Spike in Cybersecurity

Target audience: Operators of Essential **Gas** services

Means: promotional material, AR in a Box train the trainer session of OES, e-learning, e-training, delivery of dedicated sessions for dissemination

Theme: to be decided with the community

Spike in Cybersecurity

Target audience: Energy operators per NISD2 (possibly generators or renewables)

Plan next year activities based on priorities decided by the community

3 YEARS AR PLAN: HEALTH

2022

Cybersecurity First Aid

Target audience: Medical Staff of healthcare operators

Means: promotional material, AR in a Box train the trainer session of OES, e-learning, e-training, delivery of dedicated sessions for dissemination

Theme: Phishing and Cyber Hygiene
Timeline: June 2022

NISD2

2023

Cybersecurity First Aid

Target audience:
Extension to new entities under NISD2 (laboratories, research entities,etc)

Means: promotional material, AR in a Box train the trainer session of OES, e-learning, e-training, delivery of dedicated sessions for dissemination

Theme: TBD

2024

Cybersecurity First Aid

Target audience: Medical and non- medical staff

Explain the implications of implementing NISD2 – let's talk about measures

Plan next year activities based on priorities decided by the community

HEALTH CAMPAIGN 2022
FACTS AND FIGURES

- ENISA Threat Landscape 2021
  - Unpatched vulnerabilities and legacy software is particularly critical in the healthcare sector
- ENISA annual incident report under NISD
  - Healthcare is the most impacted sector
- IBM report
  - for 11 consecutive years healthcare had the highest industry cost of a breach
  - increasing 29.5% from 2020-2021
  - an average total cost of $7.13 million in 2020 to $9.23 million in 2021
- Verizon 2021 Data Breach Investigation report
  - 36% of breaches were connected to phishing attacks
  - an increase of 11% compared to the previous year

CYBER EUROPE-SNEAK PREVIEW

CYBER EUROPE LEGACY

ENISA manages the programme of pan-European exercises named “Cyber Europe”

- Organised biannually since 2010, together with Planners from MS
- This is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States
- The Cyber Europe exercises are simulations of large-scale cybersecurity incidents that escalate to become cyber crises.
- The exercises offer opportunities to analyse advanced technical cybersecurity incidents but also to deal with complex business continuity and crisis management situations.
- Cyber Europe exercises feature scenarios, inspired by real-life events and developed by European cybersecurity experts. Thus each of the exercises is effectively a flexible learning experience for the participants.
- Focus on a different Sector every year. (ex. ENERGY, ICT&CLOUD, MEDICAL)

CE2022 -SUMMARY

- 2 Day Event
- Scenario focuses on Healthcare Sector, which includes national/governmental CSIRTs, Cybersecurity Authorities, Ministries of Health, healthcare organisations (e.g. hospitals/clinics), eHealth service providers, and health insurance providers
- ISPs & Cloud Service Providers were chosen as a secondary Target to be tested
- Real-life inspired technical incidents that can be analysed using forensic and malware analysis, open source intelligence
- The incidents will build-up into a major crisis at all levels: local, organisational, national, and European. Business continuity plans and crisis management procedures will be put to the test.

18 INCIDENTS IN TOTAL

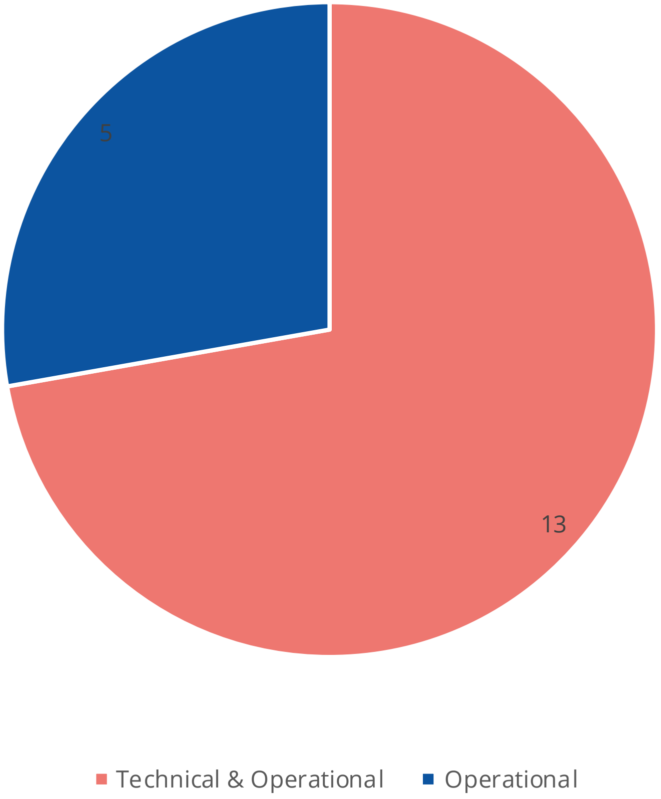
18 incidents in Total

- 5 Operational only Incidents

- 13 Technical incidents that can be played operationally as well

Types of Incidents:

Forensics, Malware Analysis, Log Analysis,
OSINT, Incident Handling, IOT Forensics, Mobile Forensics



LINKS & MEDIA

- Cyber Europe — ENISA (europa.eu)
- Cyber Europe 2022 (former CE2020) — ENISA (europa.eu)

For more information:

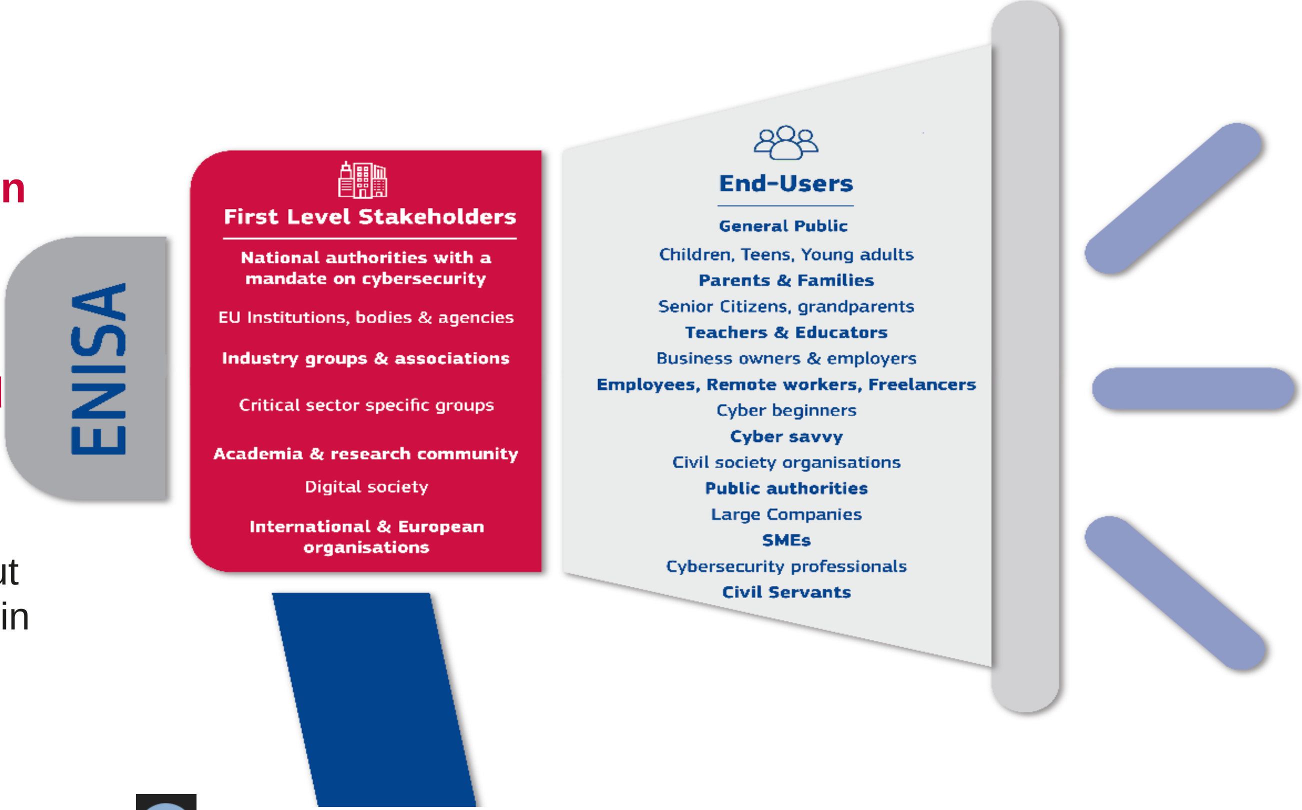
- Video trailer
- Posters
- Leaflet
- Official ENISA's social media channels

(Twitter, Facebook and LinkedIn), hashtag: #CyberEurope

COUNTING ON THE ECOSYSTEM

We are counting on you to

- ➢ **act as multipliers**
- ➢ **help us transmit the campaign messages and materials effectively and in a broader fashion**
- ➢ **reaching specific audiences**
- ➢ **at national, European and global level**



ENISA

First Level Stakeholders

National authorities with a mandate on cybersecurity

EU Institutions, bodies & agencies

Industry groups & associations

Critical sector specific groups

Academia & research community

Digital society

International & European organisations

End-Users

General Public

Children, Teens, Young adults

Parents & Families

Senior Citizens, grandparents

Teachers & Educators

Business owners & employers

Employees, Remote workers, Freelancers

Cyber beginners

Cyber savvy

Civil society organisations

Public authorities

Large Companies

SMEs

Cybersecurity professionals

Civil Servants

In case you want more details about our activities, or you are interested in working with us and being our multipliers, you can contact us at Awareness@enisa.europa.eu

or

Georgia.Bafoutsou@enisa.europa.eu or in

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 152 31
Attiki, Greece

☎ +30 28 14 40 96 55

✉ Georgia.Bafoutsou@enisa.europa.eu

🌐 www.enisa.europa.eu