Newsletter #1 | 2020

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Stakeholders' Newsletter

Thank you for joining our mailing list and be part of the EU Cybersecurity Competence Network!

CONCORDIA is a lot of things, but its soul pushes to create a pan-European community to boost our cybersecurity competencies. This newsletter is one of the services we created for you, cybersecurity experts: from industry to academia, from technical to legal, from business to society. Alone we can go fast, but only together we can go far.

Enjoy your reading, and don't hesitate to provide feedback**.**

This issue

www.concordia-h2020.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 830927.

CONCORDIA Presentation

A Cybersecurity Competence Network with leading research, technology, industrial and public competences.

CONCORDIA provides excellence and leadership in technology, processes and services to establish a user-centric EU-integrated cybersecurity ecosystem for digital sovereignty in Europe.

Follow us on social media networks!

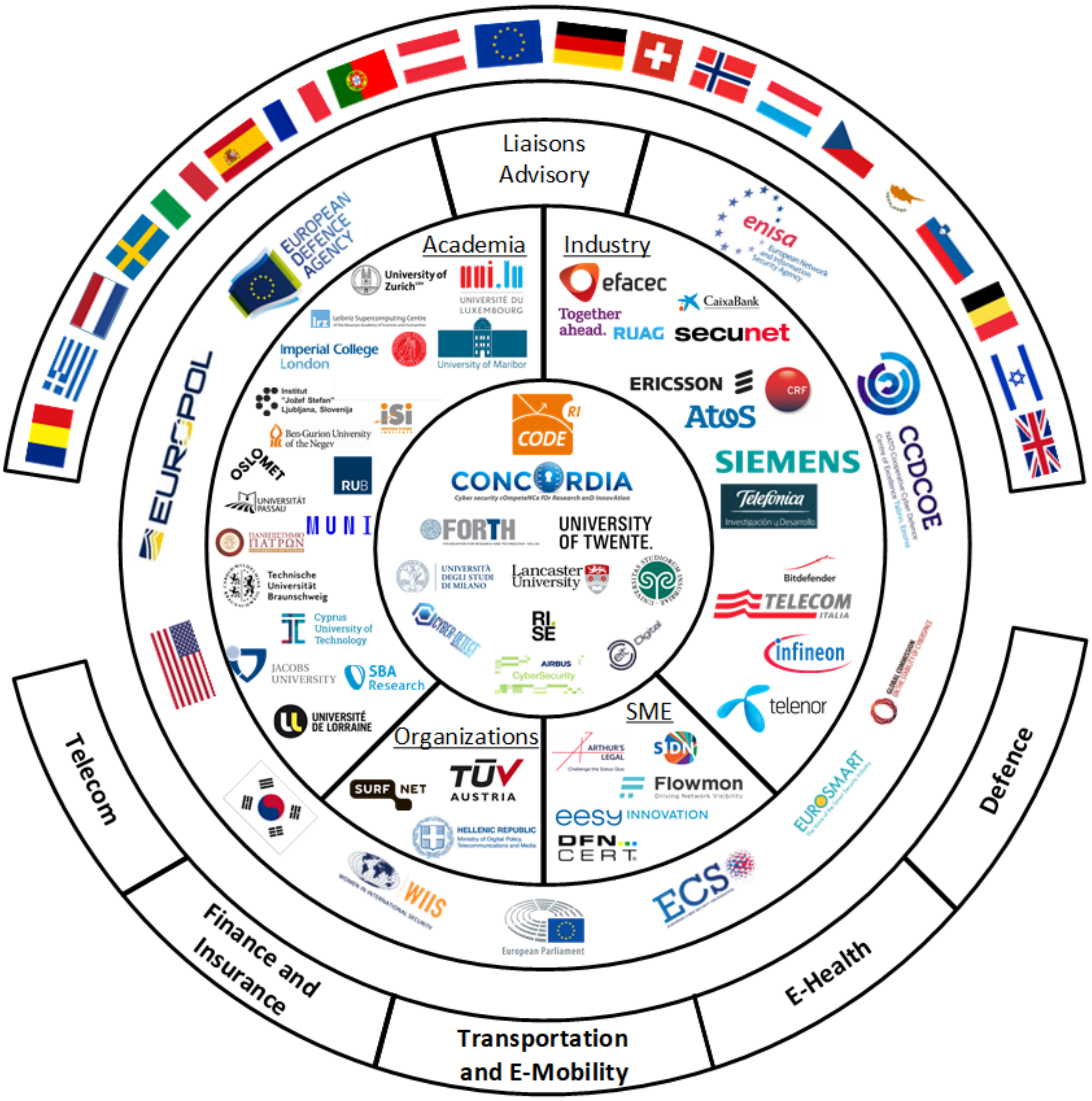
@concordiah2020

CONCORDIA Project

Concordia-h2020.eu

concordiah2020

www.concordia-h2020.eu



Suggested articles and webpages

NATIONAL CYBER SECURITY AUTHORITY OF GREECE. Covid-19 crisis and cybersecurity: Transforming the threat to an opportunity. In our more-than-ever interconnected world, we are quite aware that cyber crises cannot be contained in one’s borders, and there is a similar case with this health-related crisis. Day by day, it becomes obvious that dealing with the covid-19 crisis, follows the same lifecycle as dealing with a cyber crisis (preparation, detection & analysis, containment/eradication & recovery, post-incident activity).

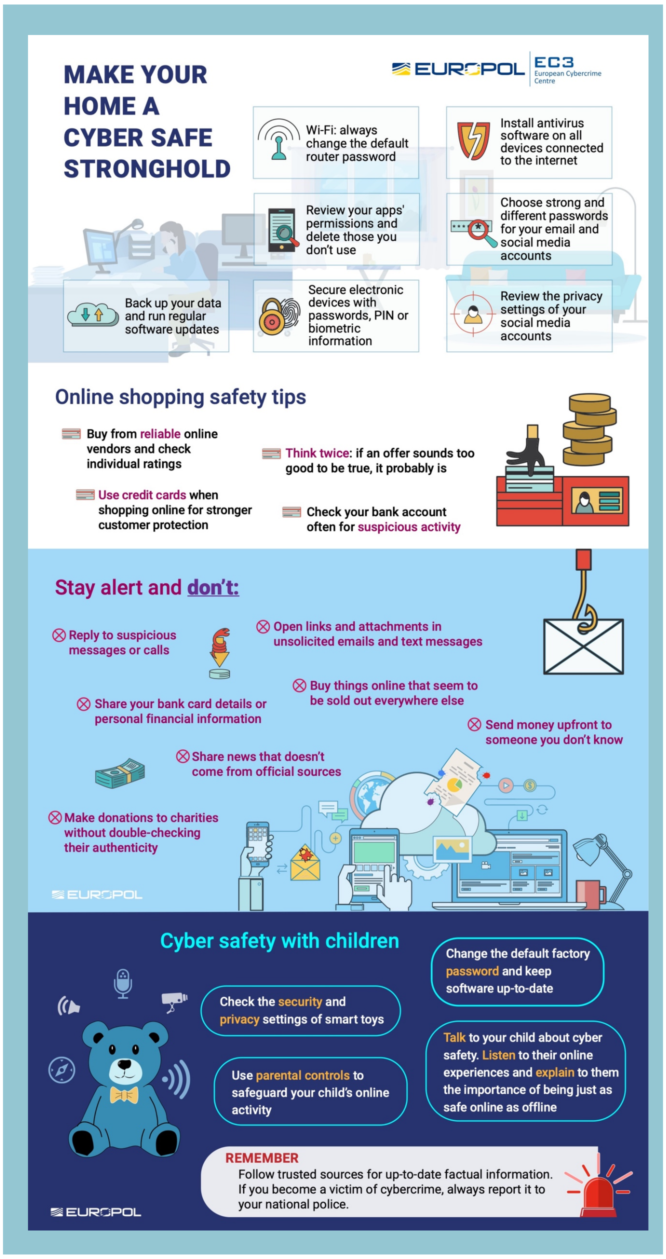
Read more at: https://www.concordia-h2020.eu/blog-post/covid-19-crisis-and-cybersecurity-transforming-the-threat-to-an-opportunity/

ERICSSON. During this global crisis, cellular connectivity has shown being a critical infrastructure societal service both for enterprises to keep business continuity and for people to stay always connected.

Read more at: https://www.ericsson.com/en/patents/articles/lessons-from-covid-19-connectivity-matters

SBA RESEARCH. Almost overnight, most companies had to severely limit physical access to their offices all over Europe. As more and more employees start working from home, connecting to their company network infrastructure, security becomes an immediate concern.

Read more at: https://www.concordia-h2020.eu/blog-post/stay-secure-during-home-office/


MAKE YOUR HOME A CYBER SAFE STRONGHOLD
EUROPOL
EC3 European Cybercrime Centre
Wi-Fi: always change the default router password
Install antivirus software on all devices connected to the internet
Review your apps' permissions and delete those you don't use
Choose strong and different passwords for your email and social media accounts
Back up your data and run regular software updates
Secure electronic devices with passwords, PIN or biometric information
Review the privacy settings of your social media accounts
Online shopping safety tips
Buy from reliable online vendors and check individual ratings
Think twice: if an offer sounds too good to be true, it probably is
Use credit cards when shopping online for stronger customer protection
Check your bank account often for suspicious activity
Stay alert and don't:
Reply to suspicious messages or calls
Open links and attachments in unsolicited emails and text messages
Buy things online that seem to be sold out everywhere else
Share your bank card details or personal financial information
Send money upfront to someone you don't know
Share news that doesn't come from official sources
Make donations to charities without double-checking their authenticity
EUROPOL
Cyber safety with children
Change the default factory password and keep software up-to-date
Check the security and privacy settings of smart toys
Talk to your child about cyber safety. Listen to their online experiences and explain to them the importance of being just as safe online as offline
Use parental controls to safeguard your child's online activity
REMEMBER
Follow trusted sources for up-to-date factual information. If you become a victim of cybercrime, always report it to your national police.
EUROPOL

Make your home a cyber safe stronghold infographic, EUROPOL
(https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know)

Enhancing Hardware Security in IoT/Embedded Systems

UNIVERSITY OF PATRAS. In an ever-expanding and fully connected world of device-centric solutions, a significant amount of IoT/Embedded systems has been deployed in a plethora of environments. This adaptation of the recent advancements of the technological field in Embedded systems these recent years can be evaluated as quite hasty, focusing mainly on performance capabilities alone, disregarding important security features.

Read more at: https://www.concordia-h2020.eu/blog-post/enhancing-hardware-security-in-iot-embedded-systems/

When Parents and Children Disagree: Diving into DNS Delegation Inconsistency

UNIVERSITY OF TWENTE, SIDN LABS, NLNET LABS, CAIDA. A key mechanism that enables the DNS to be hierarchical and distributed is the delegation of responsibility from parent to child zones. RFC1034 states that nameserver records at both parent and child should be "consistent and remain so".

Article at: https://link.springer.com/chapter/10.1007/978-3-030-44081-7_11

Stop tracking me Bro! Differential Tracking of User Demographics on Hyper-Partisan Websites

KING'S COLLEGE LONDON, BRRAVE SOFTWARE INC., TELEFONICA RESEARCH. Websites with hyper-partisan, left or right-leaning focus offer content that is typically biased towards the expectations of their target audience. Here, a first step to shed light and measure such potential differences in tracking imposed on users when visiting specific party-line's websites

Article at: https://nms.kcl.ac.uk/netsys/datasets/partisan-tracking/partisan-tracking.pdf

More cybersecurity research and innovation updates are available through CONCORDIA services

RESEARCH: https://www.concordia-h2020.eu/concordia-service-cybersecurity-research/

IMPROVEMENTS: https://www.concordia-h2020.eu/concordia-service-cybersecurity-improvements/

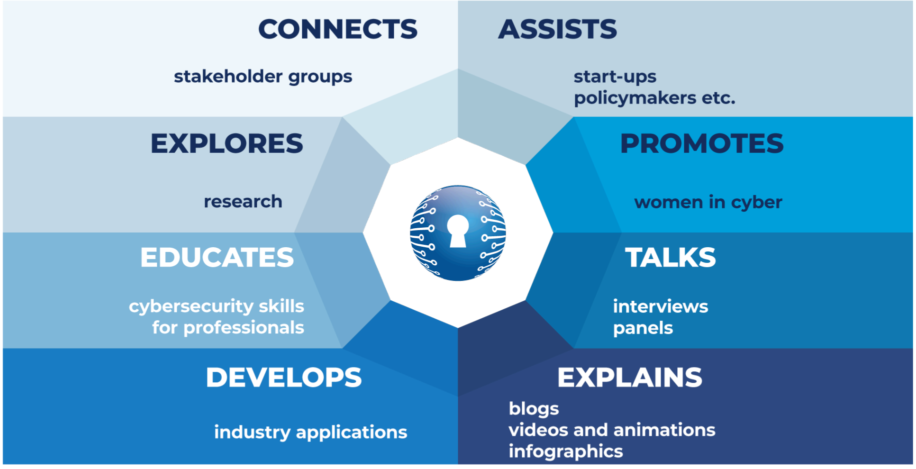
UPDATE: https://www.concordia-h2020.eu/concordia-service-cybersecurity-updates/

CONCORDIA SERVICES

Catalog and board online!

CONCORDIA aims at the continuity of its heterogeneous project outputs by disseminating them to the European cybersecurity community, but also at collecting and integrating feedback linked to the various activities of the project. CONCORDIA offers several services to its stakeholders: 15 and counting. They are organized both as a catalog or a board.

CONCORDIA service catalog (https://www.concordia-h2020.eu/concordia-service-catalog/) a path-to-follow to become a ”booster” of Cybersecurity competencies for Europe and strengthen the European sovereignty on this matter. The catalog is split in three levels, where each level implies a higher level of interaction with CONCORDIA. The first level is called *notitia* and consists of a passive interaction where the stakeholders receive or subscribe to the information provided by CONCORDIA. The second level is called *pacta* and consists of an active interaction where the stakeholders actively collaborate with CONCORDIA partners on a common topic of interest. The third and last level is *concordia* and consists in a full partnership with the stakeholders. As new partners of the consortium, the stakeholder collaborates internally to increase the value of CONCORDIA and take the lead on a specific aspect of the cybersecurity landscape.



- Updates
- Experts
- Research
- Improvements
- Skills
- Women
- Tools
- Starts-up
- Instruments
- Careers
- Promotion Pact
- Research Pact
- Industry Pact
- Community
- Partnership

CONCORDIA service board (https://www.concordia-h2020.eu/) is a clear interface to our services and it’s the main entry point to interact with the community. The services are presented in an interactive panel that shows the capabilities of CONCORDIA. Every action word maps to one or more services.

Call for Feedback

Participate in the definition of the European Cybersecurity Consultant profile

All industries have seen examples of Cyber incidents and Cybersecurity related risks have already gained their place in the relevant Risk Assessment files. In this context the role of the Cybersecurity Consultant is becoming more and more important for all types of organizations (large or small, private, public or other). A professional profile contains the knowledge and skills that a person should have in order to perform the role effectively. At this time, no specific Professional Profile has been defined for the Cybersecurity Consultant. The CONCORDIA team, through a series of procedures, has selected **90 Skills and 200 Knowledge items** from the NIST Cybersecurity Workforce Framework as relevant for the European market and has implemented them in an innovative CONCORDIA application.

We request your valuable input to rank this compilation of skills and knowledge. Please find the details on the process and the link to the app via this link.

Join us in shaping the Cybersecurity professionals Skills Certification framework and the next courses for the Cybersecurity Consultant profile

The workshop aims at collecting feedback regarding specific needs in terms of Education for Cybersecurity professionals. In view of doing so we will share with the participants our work so far in terms of **Skills Certification Schemes** and on developing courses for cybersecurity professionals while also seeking their views on the concrete pilots we plan to run together this year and targeting the Cybersecurity Consultant profile.

For details on the Agenda and the Registration process check the this link.

Threat Landscape Validation – Join our new survey!

We would like to challenge you to tell us your opinion and join our new survey! The goal of this survey is to rate the importance of the identified cybersecurity threats in the domains of interest of CONCORDIA. As part of our work **towards the definition of the CONCORDIA Cybersecurity Roadmap for Europe**, we worked on a security threat landscape identifying evolving and emerging threats in 6 domains of interest: IoT/device, network, system, data, application, user.

To assess the validity of our findings, we prepared a questionnaire this link.

Next Events and Open Calls

S&P (OAKLAND) 2021 – conference
San Francisco, California, USA - 23 to 27 May 2021
https://www.ieee-security.org/TC/SP2021/
Submission deadline: 5 June 2020

DIGILENCE 2020 – conference
Varna, Bulgaria - 30 September to 2 October 2020
http://digilience.org/
Submission deadline: 8 June 2020

USENIX 2021 – conference
Vancouver, BC, Canada - 11 to 13 August 2021
https://www.sigsac.org/ccs/CCS2020/
Submission deadline: 12 June 2020

CONCORDIA Workshop on Education for Cybersecurity Professional
Online (LifeSize) – 2 and 3 June 2020
https://www.concordia-h2020.eu/workshops/workshop-education-2020

European Commission – open calls
https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls_en
Submission deadlines: every call has its own deadline

NGI – open calls
https://www.ngi.eu/opencalls/#ngi-forward-funding
Submission deadlines: 3 June 2020

eSSIF Lab – open calls
https://essif-lab.eu/?page_id=134
Submission deadlines: 29th June 2020, 4th January 2021, and 30th June 2021

Information on **CONCORDIA Open Door (COD)**, the annual event for cybersecurity stakeholders, is coming soon. We are working to deliver the best COD2020 event, even in this uncertain global situation of CoViD-19.

Meanwhile, check out our previous edition: https://opendoor.concordia-h2020.eu/2019/index.html

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

@concordiah2020

CONCORDIA Project

Concordia-h2020.eu

concordiah2020

Thanks for your collaboration, for any questions or content recommendation please contact us:

antonioken.iannillo@uni.lu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 830927.