Cybersecurity Awareness Calendar

CYBERSECURITY SKILLS

June 2021
This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO members' and partners' solutions and services in the relevant areas to potential users.

The monthly themes for 2021 are planned as follows:

- **January** – Phishing
- **February** – Internet of Things
- **March** – Cloud Security
- **April** – Malware
- **May** – Ransomware
- **June** – Cybersecurity Skills
- **July** – Cyber Exercises
- **August** – Cybersecurity Summer School
- **September** – Mobile Devices & Bring Your Own Device (BYOD)
- **October** – Gender Diversity in Cyber
- **November** – Safe User Authentication & Password Hygiene
- **December** – Cybersecurity Trends 2022
According to the 2020 (ISC)² Cybersecurity Workforce Study, the workforce increased 25% since 2019 to a total of 3.5 million professionals worldwide. This is the first time that (ISC)² has reported a decrease in the skills gap which can be explained by an increase in new entrants to the field (700,000) and a decrease in demand due to COVID-19 - source

In October 2020, ENISA launched an Ad Hoc Expert Group on Cybersecurity Skills Framework aimed at promoting harmonisation in cybersecurity education, training, and workforce development and to develop of a common European language in the cybersecurity skills context - source

The European Commission recently launched the Digital Skills and Jobs Platform which will become a unique reference point for digital skills enabling all Europeans - citizens, businesses and public organisations - to make the most of the digital transformation of our society and economy. The platform will function jointly with the 25 national coalitions for digital skills and contribute to reaching the EU’s Digital Decade targets - source
RESOURCES FROM ECSO MEMBERS
Cybereng is a European funded project with the objective to define skills/competence and knowledge for cybersecurity engineer and manager with further development of training. The Project is funded under ERASMUS+ and started at the end of 2020.

AIT is developing requirements on a skill set for Cybersecurity Engineer and Manager for the automotive domain. Together with the project partner a corresponding set of training materials for cybersecurity engineers and managers in cooperation with ECQA for a Europe wide certificate and based on ECTS and ECVET schemas will be designed. AIT experts will in the course of the project become trainers, capable of disseminating the defined skill sets. Overall 100 pilot trainees and 10 trainers will be achieved during the project and collaboration on and knowledge exchange of the cyber security topics between the universities and companies will be supported. AIT collaborates here with Industrial Automotive and Security experts like Elektrobit, ISCN and Real Security and the academic partners VSB Technical University of Ostrava and TU Graz.
CybExer and CTF Tech are convinced that CTFs are great not only to improve the cybersecurity skills of experienced staff. Cyber ranges need to be put in good use also for educational purposes - there is growing necessity for university cyber ranges to fill the demand of skilled workforce in cyber security sector.

Next step will be nationwide event bringing young Estonian hacking enthusiasts to preliminary regional CTFs to five Estonian towns following the final competition in October 2021 in Tartu - the hometown of Tartu University. International guest teams are also invited to give the competition international flare and test the format in wider public.

CybExer Technologies provides its proprietary cyber range for nationwide 15-21 years old CTF (Capture The Flag) cyber security/hacking competition.

CybExer Technologies and CTF Tech are on the mission to bring young generation to cyber security to improve the skills and make them think about their career opportunities. The format has been previously tested to prove keen interest towards the subject.

Cyber Battle of Estonia 2021 takes raw talents and puts them on cyber security track.
Throughout the long experience in several Red Team, Incident Response and traditional security training activities, CYS4 experienced a recurring problem: SOC structures often show limited capabilities to identify attacks and stay updated to face the latest APT (Advanced Persistent Threat), which are more and more frequent. This led to the idea of developing a new product capable of delivering a new, advanced and practice-oriented training, aimed to continuously improve the skills of SOC analysts, jointly by a benchmarking and evaluation programme to detect problems in the deployed technologies (e.g.: SIEM).

You can find more information HERE.
In cybersecurity, very often people focus on hard skills such as programming, networks, regulations, directives and technologies. Many are the skills necessary to be efficient. Nevertheless, soft skills are necessary as well. In cybersecurity we cannot leverage the return of investment for transactions and this is a huge problem in a world widely dominated by profit and driven by optimisation. In fact, the attacker has the advantage to focus on the victim, decide when to attack while the defender usually does a different job and more importantly has a few seconds to respond to an attack. Therefore, creating a direct link between investments and profit is quite challenging. Of course, there is such a connection that should keep in consideration direct and indirect costs related to an incident, calculate the possibility to receive an attack and many other elements but even more important should be clear communication as it cannot leverage a clear return of investment. Therefore, not just and only hard skills such as programming and network, but also excellent soft skills like communications skill are necessary.

Exprivia offers an educational path called Exprivia CyberSecurity Academy where hard and soft skills are trained. More here.
The Global Cyber Alliance (GCA) offers free training resources that will help you improve your basic cyber hygiene and reduce your cyber risk. Some of them are part of the Cybersecurity Toolkits for Small Business and Journalists, but do not feel discouraged if you are not a SME or a journalist—basic cyber hygiene is almost identical for everyone.

Likewise, GCA’s resources include a Learning Portal where you will find well-structured courses for SMEs but also applicable to anyone interested in improving their cyberskills.

And, if you are a bit more advanced as a user, GCA also offers a complete collection of resources to protect your email with the DMARC authentication protocol, including a set-up guide available in 18 languages!

Follow us on social media (@GlobalCyberAlln, @EMEA_GCA, GCA on LinkedIn) to discover new resources and training opportunities, such as the Cyber Basics for Small Businesses training that we offered with our partners from the Cyber Readiness Institute and Mastercard last April.
Training and development in the field of IT security is an issue of national interest, given that cyberattacks on critical infrastructures or industrial complexes can result in significant financial losses, the disruption of vital supply networks, or the breakdown of public order. There is a huge demand for training in this domain. In response to this problem, Fraunhofer Academy and a select group of universities of applied sciences have developed a modular concept for cybersecurity training.

»Cybersecurity Training Lab« strengthens the skill development in the field of IT security. Joint research groups open up highly topical subject areas and convey the latest findings in innovative learning scenarios.

IT teams and managers from industry and public administration benefit from this compact qualification in high-quality laboratories with up-to-date IT infrastructure. They simulate real threat scenarios, learn their significance and consequences, and study suitable solution concepts practically in their use and efficiency.

You can find more information here.
New functions in vehicles are increasingly created through networked connections of control devices both interconnected between devices and with other external communication partners. This new complexity also creates new possibilities for attacks, thus, IT security aspects must be incorporated into vehicle development in a target-oriented manner. The seminar “IT security in Vehicle Communication” at the Fraunhofer AISEC Cybersecurity Training Lab covers the basic cryptographic mechanisms, presenting and discussing them, introducing the field of IT security in vehicle communication.

Join the English language websessions on September 23th and 30th here.

The Fraunhofer Cybersecurity Training Lab offers IT security training for everyone. Fraunhofer AISEC provides trainings with a focus on embedded systems, mobile security and Internet of Things. The high practical content in the laboratories in Garching near Munich, Nuremberg and Weiden or the online seminars enable participants to directly apply current research results in practice.
BREAKING THE BOTTLENECK OF THE INTEGRATION OF INDUSTRY AND EDUCATION IN THE CULTIVATION OF TALENT

In 2013, Huawei launched its **ICT Academy**, a school-enterprise cooperation project that involves higher education institutions, to help build that talent ecosystem incl. Cyber Security.

Huawei has held annual **ICT competition** since 2015. It does not only provide an international competition, but a communication platform for college students enrolled in Huawei ICT Academy program. Through this competition Huawei aims to challenge the students' ICT knowledge as well as practical and application skills, and ultimately, inspire innovation.
For those who are unemployed, living in Ireland and +18yo our Future in Tech programme has a Cybersecurity Analyst pathway and the next programme commences 21st June. This is a one year programme with industry relevant certification and it's free. To apply click here.

Our Certified Cyber Risk Specialist course run by ICTTF is open for applications and equips students with a comprehensive understanding of cyber risk management. The syllabus assumes a non-technical student and covers a range of topics from identification of cyber risks through to risk management options. This course is fully online and to apply click the link above.

Our Certified Cyber Risk Officer course equips students with a comprehensive understanding of cyber risk management. The course has been designed to equip students with the knowledge, skills and confidence they require in order to protect the digital assets of their organisation and support the efforts of or lead the implementation of a cyber risk framework. This is an eight week tutor led and online course which is run by ICTTF.

Today's organisations and their staff need to be aware of the potential cyber risks and threats that exist. We offer Virtual Capture The Flag (vCTF), an interactive fun environment and opportunity for organisations to have their employees engage in a set of technical or non-technical challenges which:

- trains them to both recognise and mitigate exposure to potential threats,
- ensures that they hone their cyber awareness skills through puzzles and challenges,
- tests their knowledge and competency, both individually, and as a team.

For more information go to our Virtual Capture the Flag page.

Our Cisco Networking Academy offers two free courses - Introduction to Cybersecurity (15 hours) and Cybersecurity Essentials (30 hours), both are self-paced and upon successful completion of either course, participants will have access to a branded Cisco Certificate of Completion.
In this ‘never ending digital world’ cybersecurity skills are useful for all, at school, at home, when you start a cybersecurity career, and in every kind of work. The Spanish National Cybersecurity Institute (INCIBE) helps you in all those situations:

- **For children and educators**: ‘Cybersecurity for educators’ gathers a series of materials and resources to think and apply measures and good security habits in the use of educational platforms and applications in the classroom or as a mean for remote training and learning.
- **For anyone at home**: have fun and learn cybersecurity by playing with your family and friends. Put your knowledge into practice to stop frauds or threats on the Internet and combat them with good cybersecurity practices.
- **For those who want to be a cybersecurity professional**: this infographic ‘How to became a CS professional’ helps you start in this world as a professional, showing you the steps to follow, as well as the skills you’ll need to acquire.
- **For SMEs**: a new section ‘TemáTICa - Social Engineering’ (available as of 8/06/2021) gathers resources to help employees and business owners to strengthen their human inner firewall against all kind of deceptions and manipulations tools the cybercriminals use to get access to our critical information.
One way to fix the skills gap in the cybersecurity domain is to provide more and better cybersecurity higher-education programs. However, designing a high-quality curriculum on cybersecurity can be a very difficult task due to its requirements on interdisciplinarity, hands-on training components and the lack of good practices and examples of existing programs.

Furthermore, it is very difficult for education providers to choose the actual content of cybersecurity curricula, as we currently lack a universal skills framework that would provide the descriptions of knowledge and skills required by particular positions available on a job market. As a result, many novel cybersecurity programs are designed only by small modifications of existing study programs (e.g., on Computer Science, Telecommunications, etc.), which does not sufficiently reflect the actual employers’ requirements on graduates.

INOV has been working with the SPARTA Training and Awareness team to build a diverse and inclusive cybersecurity study program, helping to gather inputs from various universities around the globe, including the Outermost Regions of Europe. To help education providers with the curricula design, SPARTA developed a simple web tool that makes it very easy to compose and analyse a cybersecurity study program. In particular, it allows users to define their own cybersecurity courses, classify them according to their content, compose the curriculum for a higher-education program and analyse if the curriculum reflects the requirements of particular work roles. Using the tool, it is simple to design new and analyse existing curricula according to the requirements of standardised frameworks.

The SPARTA Curricula Designer is publicly available [here](#) and is currently in the pilot testing phase, so feel free to design your own cybersecurity study program and let us know about your feedback!
1. Respond comprehensively to security incidents as malware, ransomware, phishing, APTs & DDoS

2. Meet regulatory guidelines as PSD2, PCI DSS, GDPR, ISO 27001 and 20000 with knowledge of security audits & compliance

3. Use analytics & intelligence to identify attacks as quickly as possible, aggregate network & application data to proactively prevent attacks

4. Handle of all types of data, including secure, encrypted transfer to cloud and collaboration tools as well as storage
Businesses need teams and staff who can work autonomously and make quick decisions even in uncertain circumstances. COVID-19 caused the mass relocation of workers from the safety of their corporate network to their bedrooms, kitchen tables or studies. Because of that, the attack surface of organisations increased exponentially. This challenge has caused security to become the top technology investment priority, and cybersecurity has become the most in-demand skill set.

The epidemic has also forced IT managers into a changed role and this trend not only continues but is complemented by the need for businesses to protect the health, safety and well-being of their employees while also adapting to a rapidly changing legal environment. This places an additional responsibility on IT managers who must ensure that measures are taken to ensure the lawfulness of data management in cooperation with the HR and Legal departments.

In this article, Security Made in LU gives some examples of possible solutions to these challenges.
WHAT DO YOU NEED TO BE SKILLED AND HAVE THE RIGHT POSTURE?

- Train, Test and Research
- Focus on immersive practice, realistic replicate, scalable
- Work on specialised use cases adapted to your domains

Discover more here.
RESOURCES FROM THE COMMUNITY
BSIDES BRUSSELS

BSides Brussels is a security conference in Brussels, Belgium, with talks and workshops. It aims to strengthen the exchange of knowledge, cooperation, communication, and integration between the different actors active in the IT security industry. The first edition of BSides Brussels will be held in May 2022. More HERE.

BruCON

BruCON is an annual security and hacker conference that provides two days of exciting atmosphere for open discussions on critical infosec issues, privacy, IT, and its cultural/technical implications on society. BruCON offers a high-quality lineup of speakers, security challenges, and workshops, as well as deep-technical training. More HERE.
The cybersecurity skills gap has left over 4 million cyber positions unfilled. See how we can provide future cyber workforce the skills they need and ready the next generation of professionals. Learn more HERE.

CYBERSKOOL

CyberSKool is a yearly conference where kids (7-15y) are taught about IT security awareness, hacking (out-of-the-box thinking and problem-solving) by doing STEAM activities, and IT skills such as coding, hardware hacking, encryption, general IT Security Awareness, etc. Exercises are given in Dutch, French, and English. More HERE.

CLOSING THE CYBER SKILLS GAP STARTS WITH EDUCATION

The cybersecurity skills gap has left over 4 million cyber positions unfilled. See how we can provide future cyber workforce the skills they need and ready the next generation of professionals. Learn more HERE.
We live in a world where threats are constantly evolving and changing, meaning cyber security is not an easy field to keep abreast of. Security practitioners need to stay in the game, develop new skills to stay ahead of the trend cycles, where advances in technology quicken the development of products and services. Level up your cyber skills with us!

INTERACTIVE PHISHING TEST FROM “EBANKING – BUT SECURE!”

Do you recognise phishing? Take the test at “EBanking – but secure!” available HERE.

WHEN IT COMES TO CYBER SECURITY, EDUCATION IS CRITICAL

Learn from the best
Endpoint protection is a key aspect of the corporate cybersecurity strategy. However, technologies are not efficient against complex cyber-attacks without constant security monitoring and analysis.

More HERE.
THANK YOU!
for your time

Cybersecurity Awareness Calendar is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

www.ecs-org.eu
secretariat@ecs-org.eu

/company/ecso-cyber-security/
@ecso_eu