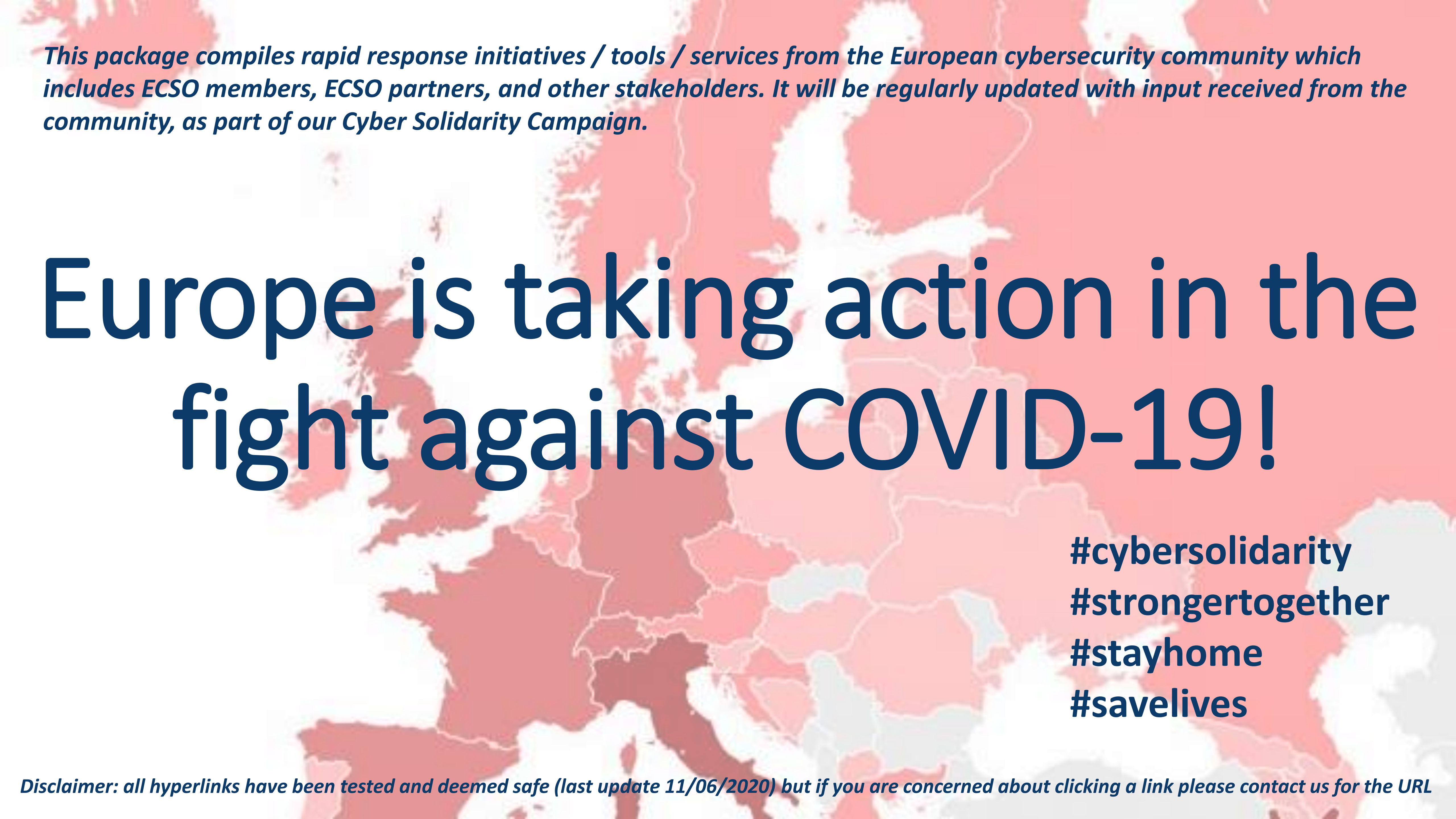
ECSO
EUROPEAN CYBER SECURITY ORGANISATION

COVID-19 CYBERSECURITY RESPONSE PACKAGE

An ECSO Cyber Solidarity Campaign

This package compiles rapid response initiatives / tools / services from the European cybersecurity community which includes ECSO members, ECSO partners, and other stakeholders. It will be regularly updated with input received from the community, as part of our Cyber Solidarity Campaign.



Europe is taking action in the fight against COVID-19!

#cybersolidarity
#strongertogether
#stayhome
#savelives

Disclaimer: all hyperlinks have been tested and deemed safe (last update 11/06/2020) but if you are concerned about clicking a link please contact us for the URL

1. Resources for the healthcare sector

2. General COVID-19 resources

3. National / regional initiatives

4. Working from home

5. Cyber attacks during COVID-19

Resources for the healthcare sector

ALIAS ROBOTICS
Robot Cybersecurity

ECS
MEMBER

Robot Security Assessments on healthcare robots

Alias Robotics can provide Robot Security Assessments on selected healthcare robots that are being used in their hospitals. They have experience working on this and in helping several hospitals in the APAC region. Alias Robotics has the expertise and would like to offer their service for free to healthcare providers across the EU.

Website

awen
COLLECTIVE

NIS compliance software Profile by Awen Collective free for healthcare in 2020

Our critical yet vulnerable health services need all the help they can get right now.
This is why Awen Collective have made the decision to offer their Profile software for free this year (2020) to all healthcare providers, and specific healthcare suppliers such as ventilator, face mask and hand sanitiser manufacturers.
Profile will help to these providers and suppliers work quickly towards lower levels of cyber risk. Freeing up time to work on more important things, and lowering the potential for disruption to society caused by cyber attacks.

More information

Bitdefender helps healthcare businesses in their fight against Coronavirus

Bitdefender offers up to 12 months of FREE enterprise grade security for ALL healthcare organisations.
This way, Bitdefender helps healthcare providers to work at full capacity on delivering care during the Coronavirus pandemic, without worrying about falling victim to the ruthless, opportunistic attacks revolving around this crisis.
Bitdefender already secures more than 5000 medical organisations.

More here

Binalyze offers 12 months full license for AIR - Automated Incident Response and Threat Hunting Platform

Binalyze supports all healthcare organisations by providing 12 months full license for its Incident Response Automation Platform. This way, healthcare organisations could respond to incidents automatically by integrating with SIEM/SOARs, performing triage and threat hunting using YARA+, decreasing the time to investigate security alerts and providing enrichment data for their Security Operations Centers.

Apply here

CEN and CENELEC make European standards available to help prevent the COVID-19 contagion

In response to the coronavirus outbreak, CEN, the European Committee for Standardization, and CENELEC, the European Committee for Electrotechnical Standardization, agreed, in collaboration with all their Members and after the urgent request from the European Commission, to make freely available a series of European standards (ENs) for medical devices and personal protective equipment used in the context of the COVID-19 pandemic.

Website

Cybersecurity support to help protect your organisation, detect threats, and respond to incidents

CV19 is a volunteer organisation setup to provide cyber support for those in need. This was setup following the outbreak of COVID19 (Corona Virus) across the world. Their focus is on Prevent and Response services to support healthcare services in the UK and Europe on a voluntary basis.

Find cyber volunteers

Proactive cyber intelligence that keeps hospitals running smoothly

CyberMDX was founded to deliver superior cyber protection to hospitals and medical centers. Focusing on medical devices, OT, and IoT, CyberMDX's solution — developed, refined and improved over years — automates distributed endpoint discovery, classification, and monitoring, along with prescriptive multi-variable risk assessment, and operational optimization insights. All this is delivered from a single fully integrated and centralized management console. Built on a foundation of 360° visibility and world-class cyber expertise, the CyberMDX solution has already been successfully deployed in hundreds healthcare facilities across the globe (North America, EMEA and APAC).

Website

Cyber4healthcare: A free cybersecurity-healthcare service

A targeted service for healthcare organizations fighting COVID19 to find, in one click, trusted, free cybersecurity assistance, provided by qualified and reputable companies. The CyberPeace Institute, an independent non-profit based in Switzerland, will process your request for assistance, anonymize it and match it with a partner company that has the right expertise and resources. When you accept a selected partner, you'll receive cybersecurity assistance targeted to your needs, free of charge

Website

Cybourn offers its security services for free to the healthcare sector

Cybourn is currently offering its security services for free for the healthcare industry. They engage proactively with hospitals or other healthcare stakeholders (labs, public institutions, NGOs) and make sure that they are not prone to cyber attacks that can disrupt operations in any way. This can range from doing security updates in current IT infrastructure all the way to installing security products to uplift levels of protection. Cybourn are vendor-independent and therefore do not have preferred vendors that they work with or impose. The Cybourn team will respond free of charge to any request to respond to ongoing security incidents for public institutions or healthcare industry.

Website

Free anti ransomware damage recovery for the healthcare sector

Drainware Systems S.L. can provide free anti ransomware damage recovery to the healthcare sector. Drainware is dedicated to the development of disruptive technology in the field of information security solutions to provide network security and endpoint to its customers. Contact them via their website or LinkedIn for more.

Website

3D printers used to create medical equipment

HP has mobilised its 3D printing teams to face the pandemic and provide support to hospitals. 1000+ 3D printed parts have already been delivered to local hospitals. HP's 3D R&D centers in Barcelona, Spain; Corvallis, Oregon; San Diego, California; and Vancouver, Washington are collaborating with partners around the world in a coordinated effort to increase production to meet the most urgent needs. Initial applications being validated and finalised for industrial production include face masks, face shields, mask adjusters, nasal swabs, hands-free door openers, and respirator part. Tips and guidelines are available for third parties on their website to create the same medical equipment.

Website

New Dutch Cyber Coalition helps hospitals with cyber incidents

Currently, the Dutch healthcare is doing everything to help our society during the corona crisis. At the same time, criminals abuse the situation by attacking healthcare institutions and healthcare providers digitally. For example by distributing ransomware or sending spam. Cyber security experts in the Netherlands think this is unacceptable and take action by uniting in the 'We Help Hospitals' coalition to protect Dutch healthcare institutions free of charge against digital attacks in times of the corona crisis.

More here

MHealth solutions for managing the COVID-19 outbreak

Given the global situation the World is facing these days due to COVID-19, many governments, companies and citizens movements have developed mHealth initiatives to keep the population informed and help manage the crisis situation. This is a preliminary, living, non-exhaustive list of some initiatives developed in Europe, compiled with high efforts within a short time frame. Applications are still coming in and are complemented by our own network efforts.

Access the list

The threat of cyberattacks on healthcare establishments during the COVID-19 pandemic

Healthcare sector targeted : what you need to know about the hackers very unusual strategy.

Orange Cyberdefense’s Epidemiology Lab has published a report on cyberattacks targeting the healthcare sector.

Read the report here

Microsoft works with healthcare organisations to protect from popular ransomware during COVID-19 crisis

As part of intensified monitoring and takedown of threats that exploit the COVID-19 crisis, Microsoft has been putting an emphasis on protecting critical services, especially hospitals. Microsoft is now making its AccountGuard threat notification service available at no cost to healthcare providers on the front lines as well as human rights and humanitarian organisations around the world. Healthcare organisations can sign up here, and human rights and humanitarian organisations can sign up here.

More here

S21Sec supports the health sector in the management of cyber incidents

S21Sec has decided to contribute to society in the fight against COVID-19 by making available to any public or private health agency its Security Incident Response team (DFIR), completely free of charge. In addition to this, S21Sec has arranged a special operation for Cyber Surveillance of the Health Sector in Spain, Portugal and Mexico. To ensure that all companies have the best possible level of protection in these difficult times, they are making available to any company that requests it at the address https://www.s21sec.com/iocs/ the possibility of subscribing to an Engagement Indicators (IoCs) notification service which allows to avoid infections before they occur.

Website

Securely

Managed Application firewall (Cloud & On-premise)

Securely offers free autonomous protection of web applications for health organisations during the pandemic. We would like to contribute to global health organisations by taking away the security and privacy tasks so they can focus on delivering care during this global challenge. Patient data will be protected at the highest level while care is given with full devotion. Let's fight this together!

Website

sweepatic SECURITY

ECS MEMBER

Sweepatic offers full platform license for free to healthcare providers

Sweepatic are offering a full platform license for FREE during the COVID-19 pandemic for all healthcare providers (e.g. hospitals) across Europe. With the Sweepatic Platform you can map, monitor and manage your attack surface 24/7 to make your organisation more cyber resilient. Any healthcare provider interested in this limited offer can enrol by leaving their contact information in the form on the dedicated page on the Sweepatic website.

Enrol here

THALES

ECS MEMBER

Thales offers its services to hospitals to help protect them from cyber attacks

After some AP-HP servers were made inaccessible for hours during an attack last Sunday, Thales has decided to offer its services to French hospitals in order to help protect them from cyber attacks.

Thales' AVS – MIS – ArtPix Mobile EZ2GO Digital Radiography System is available now to hospitals. MIS can provide Doctors with portable, connected and easy to install X-ray imagery and it is adapted for daily chest examination for COVID 19 diagnosis. Advantages compared to Stationary X-Ray rooms or CR cassettes include: No installation time, can be used straight out of the box; No need to transfer potentially infected patients to dedicated x-ray rooms; Reduces risk of cross-contamination; Image quality and the sensitivity of the system is outstanding; Image available in real time on tablet and transmitted to central server. Demo available at: https://www.youtube.com/watch?v=Vu4JWBWoKjE

News article

General COVID-19 resources

Expert perspectives on COVID-19: how to deal with it now and in the future

Accenture SA/NV (Belgium) has set up a an impact assessment webpage to understand the consequences of COVID-19 on businesses.

Practical information by experts is provided in order to better acknowledge which risks the virus is posing for the digital sector.

The webpage is updated as and when other challenges for businesses and organisations emerge.

More here

“Cybersecurity Innovation Hub” to keep on providing services to Spanish SMEs

AEI Ciberseguridad has moved its catalogue “CATYBER” on the platform “Cybersecurity Innovation Hub”.

Doing so, the group is keeping available its knowledge and experience in the field of cybersecurity to SMEs during the COVID-19 outbreak.

Read more here

AIT threat analysis and modelling platform

AIT offers a novel cybersecurity threat analysis and modelling platform called ThreatGet and would be willing to offer this to the research community, and especially for research in the healthcare sector.

More here

CERT-EU issues Cybersecurity Guidance to Survive the COVID-19 Crisis

In the context of the coronavirus outbreak, CERT-EU is taking the necessary measures to assess the cyber aspects of this occurrence. Their team established a plan to address any potential threats that may affect the cyber security and the interests of the European Union Institutions, Bodies and Agencies (EU-I)

Read the report

COVID-19
CYBER THREAT COALITION

COVID-19 Cyber Threat Coalition

As our global community strains under the weight of the coronavirus pandemic, cybercriminals are taking advantage, attacking our most critical institutions and playing on our fears and anxieties in campaigns of extortion and fraud. The COVID-19 Cyber Threat Coalition (CTC) is a global volunteer community focused on stopping these actors. We're united in our feeling that extraordinary times call for bridging traditional boundaries to operate with unity and purpose. Join the coalition in sharing pandemic related cyber threat intelligence during this time of crisis.

Join here

CY4 GATE
ELETTRONICA GROUP

ECS
MEMBER

HITS – Human Interaction Tracking System

HITS is a software platform designed to support healthcare authorities involved in the COVID-19 outbreak. The "web-based" platform is able to collect, process and aggregate geolocation data from mobile devices, thus allowing the detection of potential outbreaks of coronavirus infections that are not yet known. The processing of these data, voluntarily made available by the positive individuals, allows to trace their movements, antecedents from 2/4 weeks before the contagion. Simultaneous cross-checking of multiple tracks will allow the detection of high-risk areas through Artificial Intelligence algorithms, taking into account the simultaneous presence of multiple people who tested positive.

For further information, please contact hits@cy4gate.com

Cyber Services launches On|Cyber blog

Cybersecurity professionals at Cyber Services have launched the On|Cyber blog as an initiative to collect the clear voices in Hungary on relevant cybersecurity issues, regardless of position, occupation or employee. The blog launched 2 weeks ago received organic featured promotion from the biggest online portal in Hungary (index.hu) and various authors are working to provide relevant and up-to-date content from technical issues to digital parenting advices, all relevant for the COVID-era. The blog is delivering at least two hands-on easily understandable articles weekly to reach a wide audience.

Find the blog here

E-Learning on Cyber Hygiene available in 13 languages

In the new normality of global pandemics, the number of people relying on online security has skyrocketed. Unfortunately, cybercriminals are also aggressively taking use of the crisis . There is a steep rise of COVID-19 virus related cyber incidents – DDOS attacks, phishing, malware and data stealing apps applied. In this context, CybExer Technologies in Estonia has created cyber hygiene course for wide public use which is available in 13 languages. This is an interactive site where everybody can learn and test their cyber hygiene skills and prepare against the threats in the digital world.

Find it here

Instant Secure User Authentication with EPAS

Insecure password authentication is often exploited in order to gain access to healthcare systems, pharma research, and critical infrastructure. While there are several types of alternatives to passwords, they are often incompatible with legacy systems and take many months to deploy. The easiest and fastest way to secure user authentication is to stay with passwords and implement quality assurance. Detack is offering the proven and patented EPAS solution in a simplified, low cost version for quick installation. Deployable within 3 to 5 days, it requires little resources to operate, and provides instant detection and remediation tools against all attacks exploiting weak, leaked, or shared passwords.
Contact: cpack@detack.de

More info

Digital Skills and Jobs Coalition mobilises stakeholders to provide digital skills

The European Commission has mobilised its stakeholders in the Digital Skills and Jobs Coalition to take action to support digital skills development and share their initiative on the Commission website. The initiatives are organised according to the target group they address (i.e. schools, SMEs etc..) and where they are available. They have also launched a dedicated call for pledges asking organisations – companies, training providers across Europe – to pledge for new actions to help provide the needed digital skills in this emergency period.

Website

COVID-19
Digital Skills and Jobs Coalition
Call for Pledges
Europeans need digital skills more than ever.
Make your contribution.
pledgeviewer.eu

ECHO

European network of Cybersecurity centres and competence Hub for innovation and Operations

ECHO COVID-19 CTI Defense Alliance

The ECHO network of cybersecurity centres has joined forces to establish its COVID-19 Cyber Defence Alliance in order to support all initiatives that aim at protecting the EU member states, key services and critical infrastructure from cyberattacks. Its mission is to protect against any form of cyber attack that would take advantage of the COVID-19 crisis.

The ECHO COVID-19 Cyber Defence Alliance will define assets and vulnerabilities, identify potential attack methods and define possible mitigation measures.

More here

ENGINEERING

ECS MEMBER

Engineering's Smart Proximity solution for the new distancing rules

Smart Proximity is a new, simple and effective solution for managing the distance to work, ensuring protection of personnel and production efficiency. The wearable sensor can connect to one or more sensors nearby. Each sensor interacts with the other by sending and receiving information on proximity. When two devices are visible, they alert the user in real time, inviting them to maintain the safety distance. The device is able to detect other devices within 1.5 meters with a margin of error of +/- 10 cm. The information collected by the device is sent to a storage and processing system which analyses all the events recorded by the device and notifies you if a user is affected by COVID-19. The unique identifiers of the sensor and the relation between sensors are strictly anonymous with no link to user data. The unique identifiers are encrypted and information travels on a secure channel.

More here

Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures

EU Members States, supported by the Commission, have developed an EU toolbox for the use of mobile applications for contact tracing and warning in response to the coronavirus pandemic. This is part of a common coordinated approach to support the gradual lifting of confinement measures, as set out in a Commission Recommendation last week. Contact tracing apps can play a key role in all phases of crisis management, especially when time will be ripe to gradually lift social distancing measures. They can complement existing manual contact tracing and help interrupt the transmission chain of the virus. The toolbox is accompanied by guidance on data protection for such mobile apps.

More here

DIGITAL SME launches campaign to showcase innovative Digital Solutions to mitigate the COVID-19 crisis

European digital SMEs are offering solutions to the crisis. Browse through the digital solutions and services below to find tools that will improve your particular situation. Some SMEs are even offering their solutions free of charge during COVID-19!

Browse the list or join the campaign

Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis

The Europol report provides an overview of how criminals adapt their misdeeds to the COVID-19 pandemic. It is based on information Europol receives from the EU Member States on a 24/7 basis and intends to support Member States’ law enforcement authorities in their work.

Read the report

Free cybersecurity advice and two useful tools for Italian citizens

Exprivia, with the support of QuestIT, has developed an online virtual assistant called “Rita” to answer all questions on the Italian Decree for the COVID-19 lockdown. It can be activated for free by all public bodies who request it. Furthermore, in collaboration with the “Federazione delle Società Medico Scientifiche Italiane“ (FISM), they have also set up an app «#iorestoacasa» to help citizens self-assess their symptoms and behaviours during this epidemic outbreak.
Exprivia are also providing free advice to companies to evaluate cyber threats.

More info here

COVID-19 Cyber Intelligence Hub

This is a hub for useful, practical advice for everyone from home users and employees to seasoned cyber security specialists.

For the duration of the pandemic, F-Secure has committed to providing practical information on cyber security to everyone who needs it. We'll feature content from around the internet that helps understand and tackle the challenges that COVID-19 has created.

Access the hub

GMV puts its set of eHealth and remote consultation tools at the disposal of health authorities

Antari, GMV's suite of eHealth products and Epidemiology solutions, aims to respond to and provide a set of solutions to current health challenges; solutions in the field of chronic patient care, telemedicine systems, epidemiological control systems, tele-rehabilitation, and digital radiology systems that make use of the latest technologies in the field of health, providing solutions innovative, interoperable according to current market standards and under the strictest quality and safety standards; always from the point of view of health professionals, making technology a user-friendly tool in their professional practice.

Website

Protecting businesses against cyber threats during COVID-19 and beyond

IT teams are facing increased pressure to navigate the challenges of COVID-19. Security is a top priority and phishing is still one of the most effective methods that attackers use to compromise accounts and gain access to company data and resources. Bad actors are creating new attacks and scams every day that attempt to take advantage of the fear and uncertainty surrounding the pandemic. To help you defend against attacks, Google are sharing examples of COVID-19-related phishing and malware threats being blocking in Gmail, steps for admins to effectively deal with them, and best practices for users to avoid threats.

Read more

Free Cybersecurity support

Among many different initiatives launched, HP Inc. decided to start a campaign and offer its experience for teleworkers to let them set up home offices securely.
The service “HP Sure Click Pro” has been made available for free “for all HP and non-HP Windows 10 PC customers”.

More here

ITrust
CYBERSECURITY AS A SERVICE

ECS
MEMBER

COVID-19 Cyber Kit & tools offered free of charge as part of the current crisis

ITrust offers a COVID-19 kit with best practices guides as well as tools free of charge in response to the current crisis. This includes an EDR vulnerability scanner, antivirus, collaborative platforms, authentication tools, and much more.

Check it out

LEONARDO

ECS
MEMBER

Threat Intelligence Service for cyber defence

Starting from 6th April Leonardo is going to offer a Threat Intelligence Service against cyber threats to the first 100 applicant companies.
This service will allow the monitoring of cyber risks and related vulnerabilities.

More here

MARSH

COVID-19: Next Steps for Your Cyber Insurance

Organisations face increased cyber challenges as COVID-19 continues to spread, with core activities often disrupted or needing to be adapted. As organisations respond to changing business needs, it is vital that they continue to make cybersecurity a priority. One aspect is understanding the pandemic's implications for cyber insurance. Risk professionals should work with insurance advisors to review cyber insurance policy language. They should also refresh their awareness of all incident-response services available under their policies and how to make best use of them should an incident occur. Marsh can help review your coverage in the context of your incident-response plans and prepare the right information in light of these changing or new requests from insurers.

Website

Microsoft

ECS MEMBER

Protecting against coronavirus themed phishing attacks

While phishing and other email attacks are indeed happening, the volume of malicious emails mentioning the coronavirus is very small. Still, customers are asking what Microsoft is doing to help protect them from these types of attacks, and what they can do to better protect themselves. Microsoft therefore recaps how its automated detection and signal-sharing works to protect customers (with a specific recent example) as well as share some best practices you can use personally to stay safe from phishing attempts.

More here

Hit by a ransomware attack? Need help unlocking your digital life without paying your attackers?

Law enforcement and IT Security companies have joined forces to disrupt cybercriminal businesses with ransomware connections. The “No More Ransom” website is an initiative by the National High Tech Crime Unit of the Netherlands’ police, Europol’s European Cybercrime Centre, Kaspersky and McAfee with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

Access the website

Free access to RHEA’s MDR-Remote service

In response to the current extreme global situation, RHEA is providing a security service specifically designed for remote workers. MDR-Remote helps shield employees and organisations from today’s elevated cyber threat environment by protecting both corporate and employee owned laptop/desktop devices. Using MDR-Remote, teams can focus on their work and decision makers can focus on core operations while RHEA provides the protection, detection and response services needed. RHEA has launched a 60-day period of free access to its Managed Detection and Response (“MDRRemote”) security operations services. This is primarily offered to hospitals, other healthcare services and critical national infrastructure across the EU.

Website

ROHDE&SCHWARZ

ECS MEMBER

Application firewall in SAAS mode

Rohde & Schwarz Cybersecurity SAS has made its WAF application protection solution, R & S®Cloud Protector, available to companies free of charge, during the imposed confinement period. Building on long-standing expertise in application security, R & S®Cloud Protector effectively protects all internal and external web applications from cyber attacks without using essential internal resources. With a few clicks, application traffic can be redirected to R & S®Cloud Protector to ensure business continuity in complete security.

Access the solution

SECURITY MADEIN.LU

ECS MEMBER

COVID-19 MISP Information Sharing Community

COVID-19 MISP is a MISP instance retrofitted for a COVID-19 information sharing community, focusing on two areas of sharing: Medical information and Cyber threats related to / abusing COVID-19.

The information sharing community has a low barrier of entry, everyone can contribute and use the data. By default, the information is classified as TLP:WHITE for broader distribution and usefulness

More here

SGS

ECS MEMBER

SGS CyberLab services available to customers

Testing, Inspection and Certification continues to be important during the challenges caused by COVID-19.
SGS continues its CyberLab services for its customers. Proactive measures are implemented to ensure your interests are protected and your business needs are met. Remote auditing and inspections are available if clients studies are to be transferred. Audits can be organised using a remote inspection app allowing direct interaction with SGS experts.

Website

STORMSHIELD

ECS MEMBER

Free Network Protection and Secure Remote Access

For companies and organizations that need additional network protection or remote access capacities, Stormshield is offering licenses for its Firewall/VPN virtual appliances. These solutions, based on our EU/NATO trusted technology, can be deployed in a public/private Cloud or on-premise. As a complement to our free VPN SSL client and in partnership with TheGreenBow, we also offer licenses of the IPSEC VPN client.

Website

Swascan Domain Threat Intelligence Service

Today, the Cyber Security sector is facing many complex challenges – always increasing in number and level – from groups of very skillful Criminal Hackers, to a huge amount of data to analyse and numerous false alarms. Swascan's Domain Threat Intelligence is the solution to these problems. The process of information gathering and analysis is able to give shape to unstructured data and to connect them through concrete indicators such as level and number of vulnerabilities and the possible ways through which the Criminal Hacker could take advantage of them.

Try the service

ICT Skillnet hosting webinars & virtual CTFs to assist those impacted by COVID-19

Technology Ireland ICT Skillnet wants to help you stay up to date, feel connected and make best use of this remote working lifestyle we've all had to adapt to. Every Thursday for the months of April & May they will be holding 45 minute Lockdown Your Learnings webinars covering a multitude of topics with special guest speakers. Attendance is free but registration is required. You can register for one or more webinars at the same time.

To help you navigate the crisis, they have also launched a new bi-weekly webinar series Cyber Tech Fortnight Webinar Series as well as FREE online Capture The Flag Cybersecurity (CTF) Training Events.

Website

COVID-19: Risk Guide and Recommendations on Cybersecurity

From the point of view of cybersecurity, the current situation caused by the coronavirus is particularly worrying. Users and companies are being threatened. The CyberThreats Service of Telefónica’s SCC has divided these risks into external (those related to misinformation) and internal (those related to teleworking) risks and provides specific recommendations on how to mitigate them.

Find it here

TeleTrusT lists free IT security solutions for secure mobile working

The current switch to mobile working, home office, data transmission and remote authentication places increased demands on IT security to avoid creating new opportunities for attackers to take advantage of the moment. Not every company has the IT infrastructure to adequately secure the "home office" of its employees. In many cases, private hardware and soft. ware as well as network connections are used alternatively. It is also possible that not all components that companies and organisations make available on an ad hoc basis are state-of-the-art in terms of IT security. The members of the IT Security Association Germany (TeleTrusT) provide free IT security solutions including remote consulting via a public website for 3 months. The offers are directed to all kinds of affected users.

Find the list here

Several cloud and cybersecurity services offered by Thales

To face cyber threats in this period, Thales has decided to offer its SafeNet Trusted Access solution to secure cloud services and remote connection to corporate applications.

In addition, THALES in France is providing for free the following services during the next 3 months: Daily CERT media newsletter; Weekly Cyber Threat Intelligence reports (e.g. COVID19 cyber threat assessment, Remote / Home Office development and Cyber risks); CTI Threat reports : "RYUK - Threat to Hospitals" - Secured Messaging and Instant Messaging solutions (CITADEL) and document secured sharing solution CryptoBox by ERCOM)

Read more here & here

Remote auditing in times of COVID-19

COVID-19 poses new challenges also in the sectors of testing, inspection and certification. Therefore TÜV Nord Group has decided to offer audits via video conferences during this period of teleworking which all companies are experiencing.

Read more here

wisesecurity GLOBAL

MEE The Cybernotary

MEE the Cybernotary is a certified notification solution developed by Wise Security Global. From any device and at any time, it certifies the sending of any type of information. While this state of alarm lasts, Wise makes available to all professionals, companies and organisations that need it an unlimited credit of certified emails from its technological solution MEE the Cybernotary. With this, important communications or notifications can be made that will be registered and certified with full guarantee and legal validity: processes of employment regulation, communicated to employees, public bodies, suppliers, employment receipts, etc. From mee-thecybernotary.com access the user area, sign up and you will have unlimited credit of certified emails while the alarm state lasts.

Website

WORLD ECONOMIC FORUM

Why cybersecurity matters more than ever during the coronavirus pandemic

As the coronavirus pandemic continues to disrupt global health, economic, political and social systems, there's another unseen threat rising in the digital space: the risk of cyberattacks that prey on our increased reliance on digital tools and the uncertainty of the crisis.

The World Economic Forum offers three reasons robust cybersecurity measures matter more than ever.

Read it here

COVID-19 education response: free cybersecurity training for schools and universities

The educational platform “YesWeHackEDU” has been made available for free for 2 months for all universities and schools who request it.

This service represents the opportunity for educators and students to test their skills in cybersecurity in a period in which cybercriminals have intensified their attacks against consumers of the digital world.

Read more here

National / regional initiatives

Safeonweb.be

Guidelines on main cyber threats and security measures for citizens

The Belgian initiative Safe on Web provides information, tests and guidelines for citizens on how to stay secure online and protect oneself from cyber threats.
They have also issued COVID-19 specific guidelines and information related to phishing during the crisis.

Website

WEHELPOURHOSPITALS.BE

We Help Our Hospitals Belgium

The listed affiliated companies are ready to assist in the cybersecurity of healthcare and related sector organisations in Belgium which are involved in the battle against COVID-19. You can contact them directly to ask for their cybersecurity offerings (both preventative and in case of support during or after attacks). You can also reach out to companies(at)wehelpourhospitals.be in order to be guided to select your right partner. 3 companies most suitable to your demand will be proposed. The collective of cybersecurity companies is ready to provide help free of charge, some during the current crisis, others also beyond.

Website

BRETAGNE DÉVELOPPEMENT INNOVATION

ECS MEMBER

COVID-19 | Companies united in Brittany

In order to maintain the availability of materials, equipment, components, services and finished products which are essential for the proper functioning of health services, but also of the food industry or other vital sectors, a solidarity appeal is launched to all manufacturers, communities and other Brittany stakeholders; it is primarily personal protective equipment (PPE) that is targeted by this approach: gloves, gowns, masks, hydroalcoholic gel. To meet this challenge, this web page collects offers from companies and regional players with stocks of individual equipment or the skills and tools to produce them.

Website

HEXATRUST

CYBERSECURITY & DIGITAL TRUST

ECS MEMBER

Hexatrust members are getting mobilised against the Coronavirus

The members of the Hexatrust group are mobilising and providing support to organisations impacted by the coronavirus health crisis. The details of the products concerned and the terms of each offer are available on their website. In case of emergency, you can also contact them at contact@hexatrust.com

Website

Solidarietà digitale

Coronavirus: digitisation in support of citizens and businesses

The Digital Solidarity campaign in Italy brings together Italian companies and associations that have made and will offer free services. Discover the innovative services and solutions that can be accessed thanks to the digital solidarity initiative of the Ministry for Technological Innovation and Digitisation.

Website

We help hospitals

A platform has been set up in the Netherlands specifically for cybersecurity companies to help protect the Healthcare sector.

Find it here

TECH TEGEN CORONA

Tech against Corona: Dutch tech companies help the government

A broader initiative aiming to provide a platform for tech companies to offer their services in the fight against COVID-19. The "Tech against Corona" Initiative between Dutch tech companies offers support in the fight against the coronavirus. Numerous online meetings have taken place between tech companies / expert networks and various civil servants, including MPs. The purpose of these meetings are to discuss how these companies can support governments, aid workers, health care providers and hospitals in their fight against the coronavirus.

More here

#CiberCOVID19

The Basque Cybersecurity Centre has developed special content for the COVID-19 response which includes a dedicated COVID-19 page with infographics on "The coronavirus, used as a pretext to commit fraud and cyber attacks“; "Telework: cybersecurity decalogue“; "Security in virtual meetings“; "Tips for using cloud services“, as well as a news item on “Cybercrime uses the coronavirus to continue acting”. They have also developed a COVID-19 awareness kit with several materials available for download.

COVID-19 page

Cybersecurity Digital innovation Hub in Castilla y León

This solidarity initiative from AEI CIBERSEGURIDAD (National Cybersecurity Cluster), AETICAL (ICTs Regional Association), and ICE (Institute for Business Competitiveness of Castilla y León (a public entity devoted to promote Business Competitiveness in the region) covers needs derived from the COVID-19 crisis to support SMEs, micro-SMEs and the self-employed in Castilla y León who are using telematic services, teleworking and cybersecurity solutions as a response to the health crisis. The service includes customised response by phone and/or telematics for professionals who face technological challenges, as well specialist support for departments and qualified professionals, helping them with problem-solving skills.

More info here

#CiberCOVID19

INCIBE has launched # CiberCOVID19, a campaign with the objective of helping citizens and companies to improve their cybersecurity, providing advice and solutions. Initiatives include: For citizens: "Stay at home but cybersecure" campaign; Cybersecurity Helpline. Social Interest Phone ; For families: Cybersecurity Family Campaign and helpline; For businesses: Early warning notices related to COVID-19 and the current health emergency and state of alarm focused on citizens and companies; Articles of interest and helpline.

Website

ACADEMY OF CYBER SECURITY

Free Cyber Security & Computer Science Education for School Pupils

Free to attend, live & online cyber security school for school pupils around the world.

With 11m+ children out of school, we're providing an online cyber security & computer science education institution. Our goal is to help parents manage through the COVID-19 school lockdown whilst inspiring the next generation to explore a cutting-edge career in tech!

More here & YouTube channel

Working from home

“Syncplicity” for immediate and secure support for business continuity

Axway is offering for free its secure cloud service “Syncplicity” to let global teams access and share files online with their co-workers while teleworking. They are also promoting free training and resources for this tool.

Read more here

Recommendations on telework for both employers and employees

The COVID-19 outbreak has led to a complete transformation for many companies. Most of them are now teleworking. Nonetheless, some are experiencing issues of different kinds in organising their activities as before.

Consequently, CESIN has decided to share some tips and best practices on telework publishing an article from cybermalveillance.gouv.fr on their website.

Read more here

Cisco Supports Customers with Expansion of Free Security Offerings

Cisco Webex has expanded its free offerings to include security services for remote employees through to July 1, 2020. Those services include Cisco Umbrella to protect users from malicious websites (now free for 90 days), Duo Security to verify users' identities and establish device trust, and Cisco AnyConnect Secure Mobility Client to allow employees to work from anywhere. For the latter two, (existing customers can now exceed their user limit and new customers can get free access.

More here

Supporting small businesses during the COVID-19 outbreak

The outbreak of COVID-19 (coronavirus) is forcing teams to change where and how they work. That shift disproportionately impacts small businesses with smaller IT teams. Cloudflare protects and accelerates more than 26 million Internet properties today. Cloudflare for Teams helps some of the world's largest organizations stay productive from any location. We're making those enterprise-grade features available to small businesses at no cost.

Check it out

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

The EU Agency for Cybersecurity shares its top tips for teleworking in times of Covid-19

One of the key preventive measures for the spread of Covid-19 is social distancing. Luckily, in this increasingly connected world we can continue our professional and private lives virtually. However, with huge increases in the number of people working remotely, it is of vital importance that we also take care of our cyber hygiene. ENISA provides recommendations for teleworking and tips on phishing scams.

Read more here

EUROPOL

EC3
European Cybercrime
Centre

Make your home a cyber safe stronghold

The COVID-19 pandemic makes us especially vulnerable to cybercriminals looking to access our financial & personal data. These useful prevention & awareness tips from EC3/Europol will help you keep your home cyber secure

Read the tips

GLOBAL CYBER ALLIANCE™

ECS MEMBER

Work From Home. Secure Your Business.

Securing your business is a challenge under the best of circumstances. The new need to work remotely makes it even more challenging.

The Global Cyber Alliance has pulled together its top recommended actions from the GCA Cybersecurity Toolkit that you can implement quickly to reduce the risks associated with having a workforce that may not have been entirely ready to operate remotely

Access the toolkit and much more

LEONARDO

ECS MEMBER

Best practices to enhance Cybersecurity for all companies

Since smart working environments revealed a need to be strengthened and secured against cyber threats, Leonardo shared 12 rules to reinforce digital security for all the interested companies.

These guidelines were created to let companies understand how to provide a protected implementation of smart working for their employees.

Read more here

perseus.

ECS MEMBER

Free guidelines, info-videos and webinars on cybersecurity in the home office

The world is inevitably becoming more and more digital. Unforeseen circumstances such as the COVID-19 pandemic make digital and, above all, safe work even more important. In addition to guidelines and info-videos, Perseus has launched a series of webinars focused on offering the basic layers of cybersecurity in the home office. Their experts will impart basic knowledge and provide practical instructions on cybersecurity and data protection to you and your employees.

Check it out

Rabobank

ECS MEMBER

Rabobank remote working guidelines

Rabobank has issued a one-pager with guidelines on working from home safely, external threats, and situational awareness.

Find it here

SANS Security Awareness Work-from-Home Deployment Kit

Quickly train employees to work (and children to learn) from home safely and securely. These resources and training materials are a combination of both public resources and paid training materials which have been released for free.

Check it out

Qualtrics for remote working

Qualtrics Remote Pulse is a new platform launched by SAP to let companies/organisations understand if their employees are duly prepared to do smart working from home.
By simply putting in their contacts in this service, companies/organisations will be able to receive answers from their employees and provide them with all the suggestions they need to telework.

Read more here

Security tips for home office

Physical access to offices has been prohibited in the last weeks. This means that all companies are now setting up home work stations for their employees.

Therefore, SBA Research has provided some tips on teleworking to create a secure home office and to make sure that IT resources are available during the pandemic outbreak.

Read more here

Teleworking and precautions by SECURITYMADEIN.LU

In these times, but also in future, when performing teleworking, be it some sort of home office or working while on a mission, certain precautions should be taken to ensure a certain level in cybersecurity. In this webinar, SECURITYMADEIN.LU is discussing some practices on how to stay secure and protected.

Webinar

THALES

ECS

MEMBER

Working from home is safer with Thales' tools for free

Cyber risk has increased since the number of people starting to work from home after the outbreak of the COVID-19 pandemic.

Thales is offering 2 of its remote collaboration solutions to teleworkers for free : Citadel professional chat and call app + the Cryptobox secure telework solutions.

Read more here

Cyber attacks during COVID-19

SAFECARE

Integrated cyber-physical security for health services

Security Incidents in Healthcare Infrastructure during COVID-19 Crisis

The SAFECARE project is tracking security incidents in hospitals as the crisis progresses.

A list of recent physical and cybersecurity attacks in the healthcare sector is being regularly updated so you can keep track of trends and security incidents. Note that this list includes physical attacks, in addition to cyber-related attacks.

The consortium is available for any questions or comments regarding the listed incidents.

Find the list here

SentinelLABS

Threat Intel | Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic

Sentinel Labs have been closely tracking adversarial behaviour as it pertains to COVID-19/Coronavirus. To date, they have observed a significant number of malware campaigns, spam campaigns, and outright scams that are preying on the fears and uncertainties of the global population.

Check out their post

WebARX

COVID-19 Cyber Attacks

As a web security company, over the past weeks, WebARX has been witnessing an increased amount of website exploitation attempts. Unfortunately, many threat actors have started to abuse the panic and discomfort of the COVID-19 pandemic to conduct special crafted malware and phishing attacks worldwide. This page is a hand-curated list of the cyber attacks and threats related to the global pandemic.

Find the list here

FOR MORE INFORMATION ABOUT ECSO OR TO SHARE YOUR INITIATIVE CONTACT US

European Cyber Security Organisation
10, Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0) 27770251

E-mail:
nina.olesen@ecs-org.eu

Follow us
Twitter: @ecso_eu