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
Individuals are increasingly using their personal mobile devices for work which has only increased with the shift to remote working during COVID-19. While enabling bring-your-own-device (BYOD) can be advantageous for businesses in terms of increasing efficiency and productivity, it can also represent a significant risk. As noted in ENISA’s report on Procurement Guidelines for Cybersecurity in Hospitals, for the IT department, there is massive pressure to find a way to securely enable BYOD. Failure to do so can lead to malware outbreaks, noncompliance with regulatory requirements, and corporate exposure in the wake of personal device theft.

A recent study by Bitglass who surveyed hundreds of cybersecurity professionals across industries showed that the shift to remote work amid the pandemic resulted in 47% of organisations reporting an increase of personal devices being used for work. 82% of organisations said they now actively enable BYOD to some extent. While the use of personal devices has helped businesses improve employee productivity and satisfaction, while also reducing costs, challenges remain. The most critical concern for respondents was data leakage or loss (62%). Other apprehensions included users downloading unsafe apps or content (54%), lost or stolen devices (53%), and unauthorised access to company data and systems (51%).
RESOURCES FROM ECSO MEMBERS
The Cybersecurity Agency of Catalonia has created #NegoCibersegur, a campaign addressed to companies in order to make them learn how to keep safe against cyber attacks and to identify the main vectors of attack and entry that cybercriminals often use.

The #NegoCibersegur section shows how to turn on the protection of work devices, gives practical advice and explains good practices, especially for SMEs.

By @ciberseguracat #NegoCibersegur #ECSO #CyberAwareness
Billions of small IoT devices will change our lives and transform industries. These devices need connectivity, being installed in various remote locations, and they also need to be secure. Cellular networks, in particular 5G and NB-IoT, provide the energy-efficient connectivity and trustworthiness needed to allow small IoT devices to reliably and securely connect and communicate with other entities. The embedded SIM (eSIM) is a great candidate for these solutions, but there are also certain challenges along the way. This blog expands on the topic.

READ THE BLOG: Why eSIM standards must change for low-power IoT - Ericsson
The acronym BYOD stands for “Bring Your Own Device” that is the approach to the use of personal devices in public or private business environments. As users potentially mix their personal and professional lives on their devices, they can unintentionally expose their company to destructive cyber-attacks. The security risks of BYOD are mainly related to data protection so all the measures and the policies to implement will be related to clearly separate the work tasks from the personal tasks, leveraging on the capabilities of the devices and adopting technical solutions like the MDM tools (Mobile Device Management) that allow to implement and manage these policies, managing exceptions and violations. Almost the same challenges are to be faced by permitting personal use of corporate devices: a clear and well understanding policy has to be adopted, and an MDM tool has to be implemented to manage and monitor the device. With the same MDM technology, it will also be possible to manage access to the enterprise resources in intranet, configuring Wi-Fi and VPN, leveraging on the existing digital identity and credentials, distribute apps and remove any access or wipe the device in case of loss or stole. To prevent these risks and improve security posture in the device environment, Exprivia CyberSecurity provides various technological solutions that can be viewed HERE.
A new Android malware called Flubot is spreading in Europe. FluBot steals passwords and login information to your online accounts, personal details, and banking information. The information is used to make payments (or in other words: steal your money), account takeover and online identity theft. FluBot also sends SMS messages to new victims and spreads itself further. All of this is done without the users' knowledge.

In this blog post, learn more about the FluBot Android malware as well as F-Secure's mobile security capabilities. READ IT HERE.
September marks beginnings and reunions. The return inspires and stimulates both young and not so young, all of us with our mobile devices everywhere. This poses some risks not only for personal use. If you allow mobiles and tablets at your office or at school, take a look of these links from the Spanish National Cybersecurity Institute (INCIBE) and ‘may the cybersecurity be with you on mobility and BYOD’.

- For children and educators: Activity aimed at students to reflect on the immersion of ICT devices in the classroom and their safe and responsible use. Available here.
- At home: With these guides you will learn how to configure your mobile devices safely, through some basic guidelines to keep the information on your mobile or tablet safe from cybercriminals. Available here.
- For SME’s: If you allow your employees to work with their mobile devices recognise the risks and learn how to protect your company with this resource kit: ‘TemáTICa BYOD’. Available here.

NOTE: All resources in Spanish.
Cybersecurity incidents, like data breaches or espionage, are evolving at an enormous speed. Especially business travelers and their mobile devices face a unique risk of being targeted by cybercriminals.

At QuoIntelligence, we dedicate a full-service branch to travel risk security. Our team of geopolitical cybersecurity analysts constantly evaluates travel risks for any country in the world and adapts travel policies and briefs for our clients.

Learn [HERE](#) how you can minimise cybersecurity risks on business travels or get in touch directly.
MOBILE DEVICES & BYOD

Bring your own device (BYOD)
- No direct access to systems
- Access via remote desktop (based upon Citrix technology)

Mobile devices
Distinguish between:
- Fully managed devices (laptop)
  - Full access to all data and systems
  - Encrypted storage
- Registered devices (mobile phones / ipad)
  - MDM (Microsoft InTune)
  - Secure partition
  - Access to specific information only
  - Connected to central Identity and Access Management processes
  - Set of minimally required settings on device (including OS version, pin code length etc)
- Unregistered devices
  - No access to data
The ultimate solution to secure your terminals and mobile communications

- Local protection strong authentication & device encryption
- Communications protection voice & texts end-to-end encryption
- Internet protection all data transits via secure VPN

The most secure collaborative work solution

- Easy & secure collaboration share documents internally or with partners
- Security by design cc eal3+ | end-to-end encryption | in the cloud or on premises

The most trusted & professional audio & visio conference solution

- Secured visio conference and screen sharing simple, secured & trusted
- Design for professionals adapted, optimized, within the law for professionals
RESOURCES FROM THE COMMUNITY
Using your smartphone or laptop in a public place presents many security risks, such as the so-called “shoulder surfing” – a social engineering technique used to obtain PIN codes, passwords, and other confidential data by observing the victim over their shoulders. How to protect yourself? Read more HERE.

TAKE CARE WITH MOBILE BANKING

More than half of all e-banking transactions are carried out via a smartphone or tablet. Mobile banking offers many advantages, but also holds quite a few risks. Find out more HERE.

ARE PUBLIC PLACES SECURE ENOUGH FOR YOUR MOBILE DEVICES?
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

@ecso_eu
/company/ecso-cyber-security/