Cybersecurity Awareness Calendar

REMOTE WORKING SOLUTIONS

October 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 – Remote Working Solutions
- November – Safe User Authentication & Password Hygiene
- December – Cybersecurity Trends 2022
DID YOU KNOW?
October is Cybersecurity Awareness Month!

- ECSO’s 2020 Barometer Report on Cybersecurity in light of COVID-19 demonstrated that challenges related to remote working have been at the forefront of people's minds, with organisations needing to act swiftly to manage the need to go completely online and remote during the pandemic. This has resulted in several observed trends & challenges, including an increased need to raise awareness on cyber threats during the COVID-19 crisis, which have sought to take advantage of the pervasive shift to remote working (phishing, fraud, videoconferencing, etc.). Read the report HERE.

- ECSO has also produced a Cybersecurity Response Package during the pandemic with several resources from the cybersecurity community aimed at helping organisations and citizens with the shift to remote working. You can find the latest version HERE.

- One of the themes of this year’s European Cybersecurity Month, coordinated by ENISA, is ‘Be cyber-secure at home’. COVID is testing the online security resilience world-wide, while at the same time pushing more citizens to conduct their daily lives and work online. The main objectives of the 2021 campaign are to ensure that end-users and organisations are well informed on the potential cybersecurity risks and that they stay safe online. The general intention is to help EU citizens develop a basic understanding of the different types of online security and privacy issues. You can find more information HERE.
RESOURCES FROM ECSO MEMBERS
The Cybersecurity Agency of Catalonia presents a compilation of tips to be cybersecurity at home and stay safely among connected devices in our daily life, whether at leisure or at work.

The article provides useful information on how to protect ourselves from privacy issues in the use of wearables, IoT home automation and Smart TVs.

Read the article [HERE](#).
During the last few decades, digital security and protection have become more and more crucial. Our households and families too need protection, especially nowadays as we work remotely and connect more from home. It is important to be vigilant about cyber risks in general, and particularly how to avoid having our sensitive data exposed in all-too-frequent data breaches. Therefore, on the occasion of Cyber Security Month, APWG have prepared an infographic to offer advice on how you can make your home systems secure and resilient to cyber attacks.

Let's be 'cyber-sensible'! View the infographic HERE. Read more HERE.
Today, remote working is widely adopted by many companies for several reasons, therefore, it is necessary to have a safe and secure remote working system. The workstation must be equipped with anti-virus and anti-malware (XDR) technologies and protected with disk encrypting in case of theft or loss while in mobility. The connection used by the worker to connect with the information system is based on standard internet providers and can be protected using different technologies: from the very traditional VPN and access to internally managed Virtual Desktop Interfaces (VDI), to more innovative tools that allow a complete segregation of remote systems, the corporate infrastructure and an approach more compliant with the ZeroTrust paradigm.

Another important security factor that must be implemented to avoid identity theft is the implementation of MultiFactor Authentication (MFA) solutions. Extreme attention must be paid to the implementation of the various security measures that must not be excessively heavy for the operation, because an excess in this direction could lead workers to behaviors opposite to what is desired.

Find out about Exprivia CyberSecurity, which provides various technological solutions for remote working. Click HERE.
There are some basic steps that can be taken to secure data when working from home. Some of these 'low tech' steps are covered in the Global Cyber Alliance's blog 'Proceed with Caution: Tips for Working Remotely', which are extremely effective and free to implement!

Also free to implement is Quad9 (on laptops, Android phones, routers, etc.). All you need is to make a small change to your DNS settings (which takes less than 5 minutes) and then you are blocked from accessing known malicious websites - it really is that easy AND effective.

Finally, take a look at the resource video 'Mobile Working - Staying Safe on the Go!' for more tips and advice!

Of course you should always be following cyber hygiene best practices regardless of where you are working - the GCA Cybersecurity Toolkit for Small Business will certainly help with that!
The hybrid work environment resulting from teleworking has changed our homes and businesses, and also affects our children's education. The cybersecurity risks that threaten our families and businesses are increasingly diverse in this new paradigm of life. It is time to protect our assets and our privacy, so accept the challenge and take a look at these resources.

For children and educators: Useful resources for the secure use of educational platforms and applications, and to facilitate the implementation of cybersecurity measures even while teaching outside the educational institution. Read HERE.

At home: Learn about the main elements and recommendations for creating a cybersecure workspace with this infographic. Read HERE.

For SMEs: If you allow your employees to work remotely, the perimeter expands and they can use new applications and devices. As an employer, you need to be careful and know how to deal with the risks associated with this situation. Consult this guide: Cybersecurity in remote work, an approach guide for the business owner. Read HERE.
Many organisations have dusted off their old business continuity plans (BCP), only to find out that they haven't been kept up to date with available technologies. Unfortunately, attackers are now leveraging the fear and uncertainty caused by the spread of COVID to try to extract money and critical information from organisations and individuals. Remote working is not a challenge but a must step to keep things going. For teams who need to work remotely, some use virtual private networks (VPN) to help stay securely connected to their corporate network and applications. Other may use corporate applications that are deployed to public clouds or that are SaaS-based.

How can an organisation ensure that their house-bound and remote workers are being productive, able to access applications that today are located anywhere, from any location, over different devices, while keeping their corporate apps and information secure?

Pylones in partnership with F5 Networks provides the BIG-IP Access Policy Manager (APM) solution. APM solution delivers all of the tools that organisations need to ensure their users remain up and running, and above all, productive. APM also protects user access from all locations, over all devices. APM consolidates remote access, web access management and Identity Aware Proxy (which helps drive Zero Trust Application Access), allowing organisations to enable the form of secure application access that their organisation and users require. Read more [HERE](#).
As most of Rabobank's staff is still working out of the office, there are two solutions to stay cybersafe:

- Company supplied laptops with VPN
- Virtual workplace (Citrix)

Another important element is the use of two-factor authentication for both solutions:

- Smartcards
- RSA tokens

Last but not least, guidance on working securely has been provided to:

- Prevent shoulder surfing
- Prevent people from overhearing conversations
Work from home has become the new norm to many of us. Find out the do's and don'ts you need to keep in mind while working from home. Read more [HERE](#).
The remarkable surge in telecommuting during COVID-19 proved just how essential the possibility of working from home has become for today’s businesses and government organisations. It also highlighted the key technology known as Virtual Private Network or VPN. Thanks to VPNs, millions of employees were able to continue working on applications without undermining the security of their companies. This has been made possible thanks to the rapid deployment by companies of VPN access for all employees required to work from home. Though, beyond remote working and the standard VPN use cases inherent in nomadism and ensuring data security for business leaders and sales people, this technology offers a host of other use cases, paving the way for many new applications. Pressure on businesses from potential hackers and the tightening of data protection regulations are pushing companies to shore up their security arsenal. The development of new uses driven by 5G will clearly reinforce this security requirement. With growth in connected objects and new uses based on mobile networks, the network attack surface is set to increase very significantly in coming years for companies, which get ready to take on this heightened risk. Learn more about digital nomadism HERE and about TheGreenBow’s new ebook tackling the various VPN use cases HERE.
RESOURCES FROM THE COMMUNITY
The pandemic has led to a significant amount of people working from outside the corporate perimeters. Although working remotely has its advantages, it also exposes both employees and companies to a variety of cybersecurity risks. Discover how to keep your smart workers cyber safe [HERE](#).