ECS
EUROPEAN CYBER SECURITY ORGANISATION

OCTOBER EDITION
AWARENESS CALENDAR

Cyber hygiene & readiness

Awareness Calendar **CYBERSECURITY**

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 2022 are planned as follows:

- January – Cybersecurity certification
- February – Internet of Things
- March – Gender diversity in cyber
- April – Artificial Intelligence
- May – Cyber ranges & range-enabled services
- June – Cybersecurity for verticals
- July – Social engineering
- August – Privacy & data security
- September – Organisational resilience
- October – Cyber hygiene & readiness
- November – Cloud computing
- December – Threat & vulnerability management

DID YOU KNOW?

- October is the European Cyber Security Month (ECSM) and this year, for its 10-year anniversary, the 2022 edition of the ECSM is focusing on phishing and ransomware, with a series of activities taking place all over the EU throughout October. For this occasion, the European Commission and ENISA prepared short video messages to encourage you to get involved. Watch them here. The goal of the ECSM campaign is to strengthen the resilience of EU systems and services by enabling citizens to act as effective human firewalls and thus take a step further towards a more cybersecurity-smart society. READ MORE. #ThinkB4UClick #Choose2BeSafeOnline
- ECSO contributes with some of its own activities & initiatives that raise awareness on cybersecurity. READ MORE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM OUR MEMBERS

Professional development courses offered by (ISC)^2 to enhance cyber hygiene and organisational readiness

(ISC)^2 has courses available that can help organisations protect their network and assets and keep data secure.

Data Protection: Where Regulation Meets Practice will introduce participants to a variety of regulations and security frameworks including best practices for incorporating privacy principles into security. Incident Management: Preparation and Response can help cybersecurity professionals define a security incident, prevent an incident from becoming a breach and more.

Leveraging the Intelligence Cycle compares intelligence disciplines and discusses leveraging the Intelligence Cycle to outline the when, why and how of cyber events. Securing the Remote Workforce explores the risks and environmental issues as well as technical best practices associated with remote work.

All courses are free for (ISC)^2 members and available for purchase for non-members. For information on additional professional development courses available, visit the (ISC)^2 Professional Development Institute.

Tips for a routine with better cyber-hygiene

With cyber threats evolving constantly and dramatically, we are to consider cybersecurity proactively as part of our daily routine, as an inseparable part of our lives. Cyber-hygiene is a digital set of best practices to maintain your devices' safety, well-being and complete protection at both the personal and the organisational levels. Sustaining solid cyber-routines can not only guard your data and identity by holding attackers at bay, but it can also help to maintain your devices' functionality.

Within the context of European Cybersecurity Month, APWG.eu has prepared the following recommendations to help you improve your cyber-hygiene habits. READ MORE.

CYBER SECURITY
AGENCY OF
CATALONIA

Cyber hygiene tips for a safe and healthy digital life

On the occasion of the 10th anniversary of the European Cybersecurity Month, the Cybersecurity Agency of Catalonia, from its Safer Internet Program, has just released a new infographic with essential cyber hygiene habits.

This infographic highlights those guidelines that everyone should follow daily to minimise the risk of being hacked. Some of the key messages emphasising these principles are "Keep yourself safer with the Two-Factor Authentication (2FA)" or "Tidy your information, keep it safe".

The infographic is available in three languages: English, Spanish and Catalan. READ MORE.

By @internetambseny @ciberseguracat #ECSO #CyberAwereness
#CyberSecMonth #Choose2BeSafeOnline

Ensure credentials hygiene with DETACK

epas

Today's digital and interconnected world has created new ways to keep us all knowledgeable and safe while automating our daily lives. In recent years cybercriminals have targeted the critical infrastructure and put the lives of millions of people in danger. The use of default, weak, or already breached passwords still creates one of the most exploited vulnerabilities, despite the availability of additional authentication factors. EPAS by Detack is a patented, fully automated, appliance-based solution, that provides two main features: password quality assessments and password quality enforcement. It provides proof of compliance without requiring switching to new, alternative authentication technologies. EPAS is currently deployed in 40+ countries, for end customers and MSP/MSSP environments, serving over 5 million end users on a regular basis. No EPAS protected account has ever been breached because of an insecure password. READ MORE here and here.

Cyber hygiene and readiness: the defense of organisations

Cyber hygiene consists of the practices and precautions that users of various digital devices take to maintain and ensure that their systems function properly and securely and that their data is secure and well protected. These practices if not implemented can result in the compromise, theft, and corruption of their systems and devices. Cybersecurity readiness refers to the readiness with which an institution manages cybersecurity and all cyber threats.

Exprivia Cybersecurity has an eye always on the defense of various public and private organisations, to keep them ready at all times, at the peak of their cybersecurity readiness. Exprivia's solutions enable enterprise protection in continuous readiness, that is, the assurance of maintaining constant control over network activities and being able to react immediately.

READ MORE.

Cyber hygiene

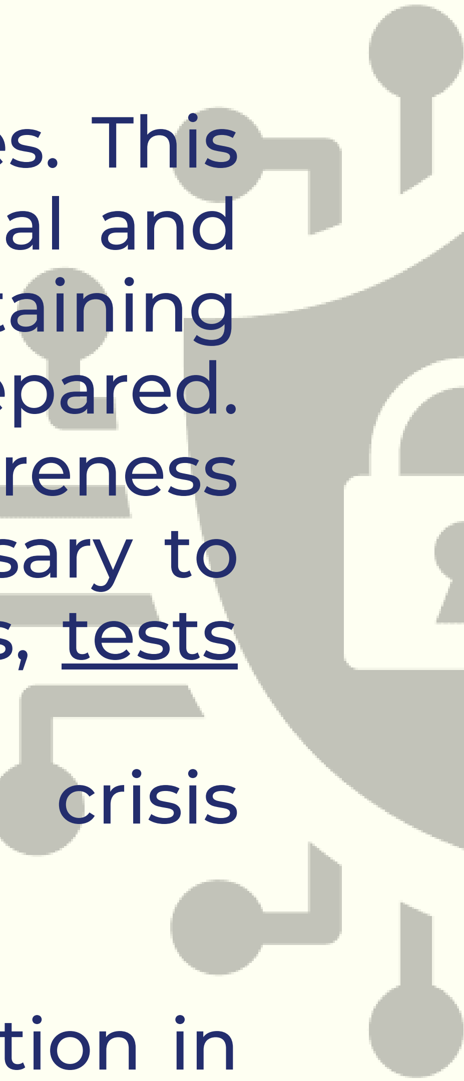
Straightforward and often free to implement cyber hygiene will protect against some of the most common forms of cyber attack. The GCA Cybersecurity Toolkit for Small Business provides free tools and resources, focused on reducing cyber risk, that any small business can implement, for free, to increase their resilience to cyber attack. The Toolkit includes the GCA Learning Portal which provides 7 self-paced mini courses to increase learning and support implementation.

Leonardo enhances customers' cyber security readiness

Organisations have to be ready to properly manage cyber security incident or crises. This requires to address a readiness phase including an assessment of the organisational and technical security measures' current state. An effective crisis management plan - containing remedial actions and all the corporate stakeholders' involvement - is to be prepared. Moreover, a cyber hygiene policy dissemination, improved by training and cyber awareness activities for specialised and non-specialised profiles, is essential. Finally, it is necessary to regularly verify processes' effectiveness and resources' awareness through exercises, tests and simulations. Leonardo supports the whole readiness phase through:

- Cyber Resilience & Consulting Services: cybersecurity risk analysis and crisis management planning;
- Cyber & Security Academy: white phishing, cyber exercise and security awareness;
- Managed Compromise Assessment Service: a complete view of the current situation in terms of potential threats or ongoing malicious activities leveraging on EDR solutions.

READ MORE: Cyber & Security Academy website, Crisis Management: people make the difference; Remote working: ready for change!



Cyber hygiene is the first line of defense.

sweepatic SECURITY

Keeping your environment clean, and safe from intruders, is an essential part of any housekeeping. It applies to your external attack surface as well. Many of your online assets are hidden, even from you. So it is of prime interest to find them – before cybercriminals do! Cyber hygiene – cleaning up your known and unknown assets – is the first line of defense.

The Sweepatic Platform continuously sweeps through your external attack surface finding all these internet-facing assets and looks for any unwanted issues and attack surface reduction candidates. The External Attack Surface Management (EASM) solution sets you up through a very intuitive and simple user interface for fast remediation so you can keep your assets nice and safe.

In short: by putting cyber hygiene first, the Sweepatic Platform helps you keep all your websites, domains, hosts and certificates and much more out of harm's way. READ MORE.

Cybercrime is a significant challenge for businesses globally.

Evolving cybersecurity threats seek out weak points in the organisation, target organisational data or the disruption of day to day operations. A solid cybersecurity risk management programme helps business leader's readiness by enabling them to assess the current security posture, determine potential dangers and implement strategies ensuring the safety and security of business information and infrastructure.

An effective risk management programme helps create the right security policies to comply with regulatory body requirements and increasingly customer requirements. In effect, it helps protect your company's reputation in the marketplace.

Technology Ireland ICT Skillnet partner with the International Cybersecurity Threat Task Force (ICTTF) offering the Certified Cyber Risk Officer and Certified Cyber Risk Specialist courses aimed at helping business leaders understand and identify potential threats and implement strategies to eliminate vulnerabilities. Cybersecurity risk management is strategically important for every business. The following Programmes in Partnership with ICTTF are offered on a regular basis: Certified Cyber Risk Officer Course; Certified Cyber Risk Specialist Course; Related course: NIST Cyber Security Expert Course

RESOURCES FROM THE COMMUNITY

EU IoT security getting stricter. Are you ready? Act now!

binaré

The European Union published the EU Cyber Resilience Act, a draft legislation related to IoT security, requiring manufacturers of smart devices to take product security measures more seriously. Be cyber proactive and read Binare's blog post "Happy World Standards Day!" to find out how Binare's platform can help IoT device manufacturers, businesses and government organisations on their way towards IoT cybersecurity standards and regulation compliance and discover cybersecurity standards. Binare's platform will check your IoT device for compliance.

Cyber hygiene

itrainsec

Cyber hygiene should never be ignored, as many breaches result from basic, and totally avoidable errors. Threat actors are notorious for aiming at the ‘low hanging fruit’, or organisations that don’t pay attention to these basic security hygiene practices, the very ones that could protect them from a wide range of attacks. READ MORE.

10 tips to minimise cybersecurity risks

In an increasingly digital world, the topic of cybersecurity has become more and more relevant, both at home and at work. However, as the use of internet-connected systems increases, so does the risk of being the target for cyber attacks. That is why it is important to follow a few practices to minimise these threats. Find out Sababa's cybersecurity tips. READ MORE.

THANK YOU

for your time!

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

in company/ecso-cyber-security

@ecso_eu

www.ecs-org.eu 🌐

secretariat@ecs-org.eu ✉