ECS
EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity Awareness Calendar

PHISHING

January 2021

Awareness Calendar

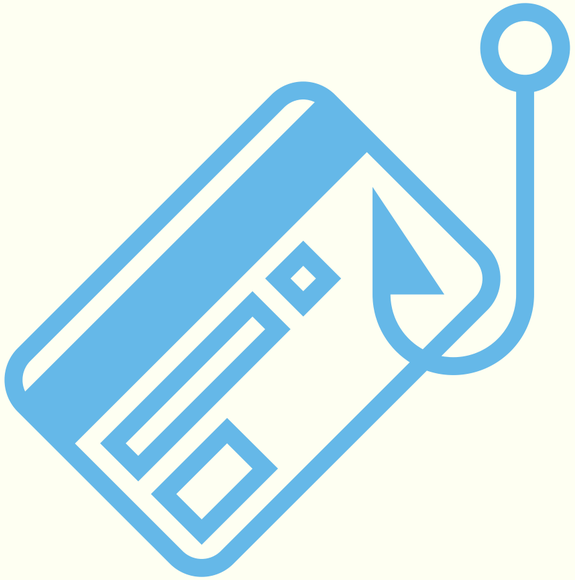
CYBERSECURITY

This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO members' 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 – Safer User Authentication & Password Hygiene
- December – Cybersecurity Trends 2022

DID YOU KNOW?



Facts & Figures about phishing

- According to Deloitte, 91% of all cyber attacks begin with a phishing email - source
- ENISA's 2020 Threat Landscape Report on Phishing found that there was 667% increase in phishing scams in only 1 month during the COVID-19 pandemic - source
- COVID-19 is now possibly the most exploited topic in phishing history - source

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

The most common
DIGITAL FRAUD METHODS

Nowadays we spend much more time online. Despite all its advantages, cybercriminals are taking advantage of this new paradigm. Within the campaign Stop Fraud Digital #STOPFraudigital, an infographic has been prepared (in Catalan, Spanish and English) on the most common methods of digital fraud. This has been made possible by the joint work of the Internet Segura program of the Cybersecurity Agency of Catalonia and the ANTI-PHISHING WORKING GROUP EUROPEAN FOUNDATION.

By @internetambseny @apwg_eu #THINKB4UCLICK #StopFrauDigital

MORE INFO:
Infographic in English
Infographic in Catalan
Video in Catalan

Phishing attacks:

AN EASY AND VERY DANGEROUS TECHNIQUE

Phishing 2020 continues to be the preferred attack technique by cybercriminals. According to Exprivia Threat Intelligence Report 3Q2020, in the 3rd quarter of 2020, 62 phishing campaigns were analysed in Italy with a total of 138 since the beginning of 2020. Industries most impacted are Finance, Healthcare, Industry and Public Administration. Phishing begins with an email or other fraudulent communication sent for the purpose of attracting a victim. The message appears to come from a reliable sender. If the deception is successful, the victim is urged to provide confidential information, often on a scam website. Sometimes, malware is also downloaded to the victim's computer. Sometimes it is enough for hackers to obtain victim's credit card information or other personal data for profit. Other times, phishing emails are sent to obtain employee login credentials or other information to perform a more sophisticated attack against a specific company.

Cyber-attacks such as persistent advanced threats (APT) and ransomware often begin with phishing. One of the most important way to protect an organisation from phishing is to increase the awareness and the culture of cybersecurity. Education should involve all employees. Senior executives are often the target of phishing campaign. Exprivia provides a large catalogue of courses with the aim of improving awareness and competence to reduce the risk of a Cybersecurity incident and limit the consequent damages.

The Exprivia course catalogue is available here

Beware of

SPEAR PHISHING EMAILS

Fraunhofer FKIE

On a Monday morning, before having a cup of coffee, an employee is changing the password for his accounts. He received an E-Mail from a colleague from IT who told him to do so. The E-Mail sounded very urgent, so he wanted to do it right away. However, the originator of the E-Mail was not the colleague from IT but an attacker who has crafted a spear phishing E-Mail. This type of phishing mail have has become very hard to identify.

In an easy-to understand workshop, our trainer shows how an attacker crafts these types of E-Mails.
What is the goal of the attacker? What is the difference between phishing and spear phishing? Which technical methods are commonly used? Our trainer shows examples of forged addresses and domains.

The goal of the workshop is to show the participants how an attacker thinks, and to enhance the chance of detecting a phishing attempt.

MORE INFO:
Here

Blog post on
PHISHING

Phishing is an online threat that doesn't seem to go away, in particular, because it has been very effective. F-Secure's H1 2020 Attack Landscape report has indicated that email still remains the preferred method for malicious threat actors for delivering spam, phishing and other malicious content.
The current pandemic that is going on in the real world has not changed or slowed down the pace of malicious threat activities in the cyber world. Phishing emails remain rampant, and with most organisation infrastructures shifting to cloud and with the proliferation of remote work and studies, the phishing themes have also shifted to target credentials of those tools and platforms.
In this post, F-Secure reviews the statistics of the phishing emails we have seen since October 2020.

Read the blog post here

perseus.
Cybersecurity to the point

During COVID-19 Lockdown:

EVERY SECOND CYBER ATTACK WAS PHISHING

Whether there is a pandemic or not, there is no slowing down when it comes to cyber attacks. Since the nationwide lockdown in Germany in mid March 2019, every fifth employee has been affected by a cyber attack. 50 % of these were caused by phishing.

Hackers have quickly adapted to the current situation and used recent events and happenings to execute their attacks by, for example, imitating official notifications and emails by organisations and financial institutions concerning COVID-19 relief benefits and support programs. The best way to protect companies from phishing attacks is to involve the employees in the process early on and to sensitise them for cyber risks.

Perseus supports companies in the process to achieve a change of behaviour among their employees by providing a long-lasting and continuous learning and awareness programme. Perseus' phishing training combines theory with practical everyday examples, thus enabling the sustainable development of an understanding of phishing and supports a positive behavioural change in the long term. More information about Perseus' phishing awareness offering can be found here

Threat Intelligence

SERVICE TO COUNTER THREATS

Intelligence driven cybersecurity strategies permit anticipating to malicious activity and prevent loss of reputation & disruption of the business processes. More than 25 experts in different disciplines, intelligence insights in an actionable Database, proprietary technology. Worldwide CTIU with access to privileged sources. S21sec is preferred collaborator of main global law enforcement agencies (Europol, FBI, Guardia Civil, etc...). S21sec Threat intelligence proposal covers fully the intelligence lifecycle (strategically, tactically & operationally) observing:

- Detection and response: Affecting the persons, VIPs, reputation and the assets of your daily operation.
- Reporting: of the threats affecting the nature of your business or ad-hoc reporting
- Enrichment: enable your security devices and services to detect the most updated threats by using unique IoCs

MORE INFO:
S21Sec's Cyber Threat Intelligence Unit

SECURITY MADEIN.LU

circl.lu cases.lu c3.lu

The most common cyber threat and the everlasting fight against it:

PHISHING

MORE INFO:
Here

If your mailbox needs some Oxygen

USE SPAMBEE

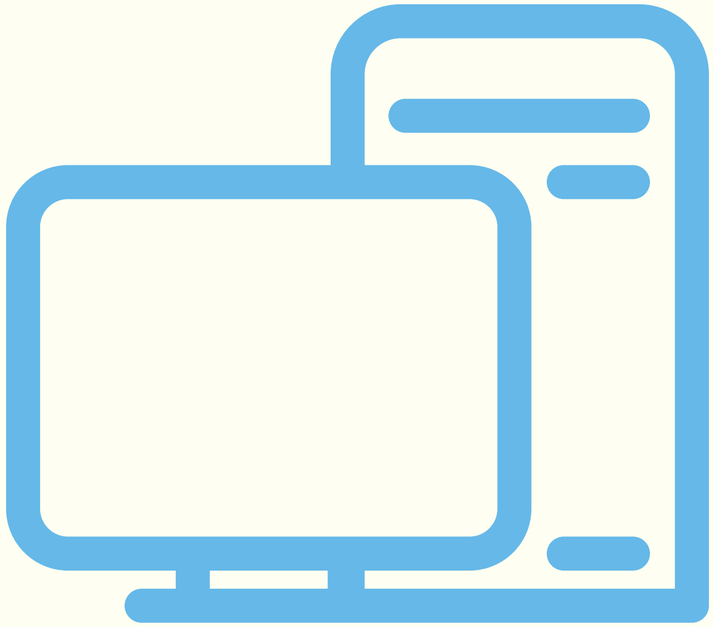
SPAMBEE is a tool that allows you to easily handle suspicious emails and notify experts of them who will make a complete diagnosis of each transmitted email. Once processed, these emails will feed a database of senders to be banned. This "blacklist" will be shared with all SPAMBEE users. In this way, the anti-spam filter will be enhanced thanks to the participation of each user.

Check it out HERE !

ECS
EUROPEAN CYBER SECURITY ORGANISATION

THANK YOU!

for your time



Cybersecurity Awareness Calendar is an initiative launched by:

European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

http:// www.ecs-org.eu

/company/ecso-cyber-security/

secretariat@ecs-org.eu

@ecso_eu