Cybersecurity Awareness
Calendar
SAFER USER AUTHENTICATION & PASSWORD HYGIENE
November 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 2022
DID YOU KNOW?

There are many ways to steal a password, as indicated by ENISA:

- Social Engineering attacks, such as phishing credentials using fake pages, voice phishing (so-called Vishing), shoulder surfing (e.g. peeping behind a person who is typing their password on a laptop) and even retrieving handwritten passwords from post-it notes.
- Stealing using specialised software or physical keyloggers. Some of these attacks require a physical presence or proximity to a laptop or a device.
- By intercepting communications, using fake access points or by leveraging man-in-the-middle attacks (MiTM) at a network level, more prevalent in public WiFis found in hotels, cafés, airports, etc.
- Brute-force attacks on passwords by trying all the combinations, dictionary attacks or by simply guessing the password.
- Retrieving passwords directly from data breaches and leveraging them using password spraying techniques to other legitimate services.

For more information and recommendations on how to improve password security check out ENISA's page on secure user authentication.
RESOURCES FROM ECSO MEMBERS
WHAT DO WE KNOW ABOUT USER AUTHENTICATION IN SECURITY SYSTEMS? HOW MANY TYPES OF USER AUTHENTICATION ARE THERE?

The Cybersecurity Agency of Catalonia, through the Safer Internet Program, is publishing an article on the different types of user authentication existing nowadays to make them well-known to citizens.

With an infographic showing all authentication types and methods, the piece on identity and access management also addresses the question of two-factor verification: reinforced safer systems that require a combination of a minimum of two independent elements to check the user identity.

The article and infographic are available in Catalan HERE.
The Robot Immune System (RIS) is a security compliant software that protects robots and robot components against malware.

Inspired by nature, it gets installed directly into your robotic system delivering an integrated suite of protection technologies. Amongst them, safe user authentication is warranted, extremely relevant even in air-gapped industrial environments. RIS is totally compatible with other OT security solutions and systems.

Want to improve your overall robot security position? Read more on our professional services HERE and HERE.
Today's digital and interconnected world has created new ways to keep us all knowledgeable and safe while automating our daily lives. In the last years the cybercriminals have targeted the critical infrastructure. The attackers using various vulnerabilities can remotely invade into a target or device, intercept traffic, launch denial of service attacks, and take control of IoT devices to create botnets. The use of default and weak passwords in this environment creates one of the most used vulnerabilities. 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 30+ countries, for end customers and MSP/MSSP environments, serving 4-4.5 million end users on a regular basis.

Read more HERE.
PROTECTING ONLINE ACCESS

Do you lock your door when you leave your home?

You should also protect your devices and online access against access by strangers the same way. Use strong passwords and two-factor authentication.

Read more HERE.
Account takeover means that someone gets unauthorised access to your online account. [HERE](#) is a classic example of account takeover.

How good (or bad) is your password hygiene? Find out [HERE](#).

The walking breach: How data breached put people at risk of cyber crime. Read more [HERE](#).
How do you shut your front door when you go out? Do you just pull it to or lock it securely? Which windows do you open on a sunny day? Apply the same logic in the online world as you do in the physical one. Our blog Bad Habits STOP RIGHT HERE explains the importance of using strong passwords and two-factor (or multi-factor) authentication. Our 10 minute mini course provides more guidance, and the free tools in the Beyond Simple Passwords Toolbox of the GCA Cybersecurity Toolkit help you implement better password hygiene and safer user authentication.

And, if you have a house or an office full of smart gadgets, you'd better change their default passwords and keep them properly patched. Read this blog on the importance of keeping good password hygiene also on your IoT devices.
By their very nature, control centres are the most sensitive element in operational infrastructures. However, control centres have very specific characteristics, which prevent the application of solutions that are commonplace in almost any other IT infrastructure. User authentication and authorisation is a clear example. In control centres, computers need to be always on, showing telemetry data, so that operators can immediately spot and react to any anomaly. 24/7 operations also require non interruptible monitoring and shift change as smooth as possible.

Consequently, generic accounts for controllers or operators can be preferred to individual accounts and authentication mechanism limited to the minimum. Biolock is a solution specifically targeted towards allowing user authentication and traceability at control centres. The solution allows to maintain workstations always visible with telemetry data while blocking any interaction until an authorised user authenticates. Several authentication mechanisms are allowed.

Read more HERE.
Authentication and password security are still extremely necessary in the digital environment. Although the use of two-factor authentication and biometric techniques such as fingerprint or facial recognition is on the rise, we should not neglect basic measures such as creating strong passwords, having a different password for each application and changing them frequently. Take a look at this resources and keep authentication secure.

For children and educators: step-by-step for password generation as part of teachers' cybersecurity routine. Read more [HERE](#).

At home: Learn everything you need to know about passwords to keep your information safe and prevent third parties from accessing it. Read more [HERE](#).

For SMEs. Read more [HERE](#).
It is a new working day. Time to wake up and get prepared.

One may first log into a social network to check the news, access some messaging applications and look for pending comments. When commuting, we may also check the maps application. Later we log into the mailbox and to a myriad of services in order to work. At the end of the day, there is some time off, maybe to access a streaming platform or some gaming cloud.

All of these have something in common: we are continuously authenticating to access services. The more accounts we own (or rather, the more we rely on them), the more we should follow proper authentication best practices.

Good authentication hygiene and knowledge are essential for your security. Read more HERE.
SAFE USER @ RABOBANK

Rabobank offers the following services:

- Client access
- Access via 2fa only
- Keep business banking as safe as possible – Rabobank. Read more HERE.
- Online banking (rabobank.com). Read more HERE.
- Employee access
- Mostly authentication based upon 2fa (smartcards)
- Where passwords are still used, check on strong passwords including well-known words
- Remote access only via VPN with 2fa
- Privileged access: accounts held in central vault with 2fa access control
- For other accounts: use of a private password solution
ALL YOU WANTED TO KNOW ABOUT PASSWORDS. BUT DO THEY MATTER AT ALL?

“If I wanted to see your e-mails or your wife's phone, all I have to do is use intercepts. I can get your e-mails, passwords, phone records, credit cards.” - Edward Snowden

The word ‘authentication’ may seem a bit abstract, mystical or mysterious, but we authenticate ourselves several times a day without even thinking or knowing about it. We authenticate ourselves when we open a door with a key, visit a library with a library card, use our passport at the border or prove our identity to a police officer if we are stopped.

Read the full article HERE.
RESOURCES FROM THE COMMUNITY
Smartphones keep sensitive personal and work-related information. Therefore, it is important to defend it and prevent it from getting into the wrong hands. To avoid strangers unlocking your mobile phone, it is essential to set a screen lock, whether it involves a pin, a password, the fingerprint or a particular pattern. Find out more [HERE](#).

**LOCK SCREEN TECHNOLOGIES FOR SMARTPHONES**

Do you work with identity-based access to information (e.g. SSO) or are you still working with an application-based access system that needs an individual password per software or device? No matter if you are working with several passwords or only a few, you need to ensure that they are not only secure but also handled safely – especially if third parties are involved. In this article we shine a light on additional factors that impact password safety and share tips to help ensure that your passwords are as secure as possible. Read more [HERE](#).

**BAD TREATMENT OF GOOD PASSWORDS**

Do you work with identity-based access to information (e.g. SSO) or are you still working with an application-based access system that needs an individual password per software or device? No matter if you are working with several passwords or only a few, you need to ensure that they are not only secure but also handled safely – especially if third parties are involved. In this article we shine a light on additional factors that impact password safety and share tips to help ensure that your passwords are as secure as possible. Read more [HERE](#).
FORGOT YOUR PASSWORD? TAKING OVER USER ACCOUNTS KAMINSKY STYLE!

In internal security assessments, it is common practice to exploit the "Forgot password?" feature of internal web applications to obtain a password reset URLs in e-mails. Timo Longin, Associate Security Consultant at SEC Consult, made an attempt to apply this concept to a web application on the Internet. Therefore, he analysed 146 web applications for vulnerabilities in their DNS name resolution and discovered that some web applications are still vulnerable today. Read more HERE.

FUTURE AUTHENTICATION FOR OUR EVERYDAY LIFE

In times of digitalisation, increasing cybercrime and data protection awareness, secure and intuitive authentication methods are needed. The XignIn authentication solution uniquely combines the highest level of security with the simplest handling for all application areas equally - without any password or additional hardware. Benefit from the wide range of application scenarios in everyday life and effectively protect your sensitive data. Find out more HERE.
THANK YOU for your time

The 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
/company/ecso-cyber-security/
@ecso_eu