WEEKLY BULLETIN
19-23 JUN 2023

Quote

"Cyber security is a social responsibility. We all have a role to play."

of the week

Cyber security in the banking sector

"Social Security, bank account and credit card numbers aren't just data. In the wrong hands they can wipe out someone's life savings, destroy their credit and cause financial ruin."

Melissa Bean

With the ever-increasing of banking services, cyber security awareness of this sector is a critical process.
Around the world, banks and financial institutions are frequent targets of cyber attacks; such as hacking customer data, identity theft, financial fraud and exploiting weaknesses in their information infrastructure.
Precisely, the banking sector has been in an increased attention of AKCESK this week, to intensify cooperation in terms of awareness and increased vigilance, in function of cyber protection of information infrastructures.
The prioritization of capacity building and the exchange of information in real time have been part of the daily discussions and meetings that AKCESK has held this week with this sector.

"We are there, together with you, to answer you 24/7 and to address all your issues related to cyber security" - said the General Director of the authority, in the meetings directed by him.

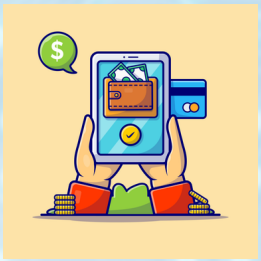
"Our mission is clear; together to build a safe cyber ecosystem for everyone, in Albania"

Advices to keep your financial information safe

1. Don't share your secrets.
Do not give your Social Security number or account information to anyone who contacts you online or over the phone. Protect your PINs and passwords and do not share them with anyone.

2. Shred papers with sensitive content.
Shred unused receipts, bank statements and credit card offers before tossing them.

3. Use the online banking platform to protect yourself.
Regularly monitor your financial accounts for fraudulent transactions.



4. Monitor your credit report.
Order a free copy of your credit report every four months

5. Protect your computer.

Make sure the antivirus on your computer is active and up to date. When conducting business online, make sure your browser's wrench icon oe padlock is active. Also look for an "s" after "http" to make sure the website is secure.

Rruga "Papa Gjon Pali II", No.3 info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039

WEEKLY BULLETIN

19-23 JUN 2023

Quote of the week

"Cyber security is a social responsibility. We all have a role to play."

Content:

Hackers target Linux SSH servers using Tsunami DDoS attacks

An attack campaign has recently been discovered where misconfigured Linux SSH servers are being targeted by being attacked with the Tsunami DDoS Bot.
When users use basic information such as username and password, Linux can allow an outsider to log into the system by brute-force guessing or using a pre-prepared list of common passwords.
Once inside the system, the attacker executes a command to download various types of malware. One of the malware installed is a script called the "key" file, which acts as a downloader and installs more malware.

It is advised for all Linux users to use strong passwords or SSH keys to protect against attacks as well as take the necessary steps to restrict access to the server by allowing only a specific range of IP addresses.

Link: Read more

Trojanized Super Mario game used to install Windows malware

A trojanized installer for the popular game Super Mario 3: Mario Forever for Windows has infected the devices of many players with multiple malware infections. The infected game has been promoted on gaming forums, social media groups enabling installation by many players. The stolen data includes information stored in web browsers, such as passwords and stored cookies containing credentials for Discord, Minecraft, Roblox, and Telegram.
It is advised to all game lovers that when downloading games or any software, make sure to do so from official sources such as the publisher's website or trusted digital content distribution platforms.

Always scan downloaded executables using your antivirus program before launching them and keep your security tools up to date.

Link: Read more

Over 100,000 ChatGPT accounts stolen through malware attacks

More than 101,000 ChatGPT user accounts have been stolen by malware attacks, according to darkweb data
These types of malware are known to steal credentials stored in web browsers by extracting them from the SQLite database. These credentials, and other stolen data, are used by the attacker for malicious purposes.

It is advised that those working with extremely sensitive information should not trust its entry to any cloud-based service, but only to locally built, self-hosted secured tools.

Link: Read more

PATCHING ALERT

Security update from Fortinet Company on a vulnerability rated as critical

Cybersecurity solutions company Fortinet has updated a vulnerability that attackers can use to execute code and commands.

The vulnerability identified as CVE-2023-33299 is rated as critical and can lead to remote code execution.

The company has not provided any advice on mitigating the flaw, so the recommended action is to apply available security updates.

Link:Read more

Rruga "Papa Gjon Pali II", No.3 info@cesk.gov.al

Autoriteti Kombëtar për CESK

autoriteti_kombetar_cesk

+35542221039