WEEKLY BULLETIN
10-14 JULY 2023

Quote of the week

"When functionality is all that matters, security is often overlooked."

Contetn:

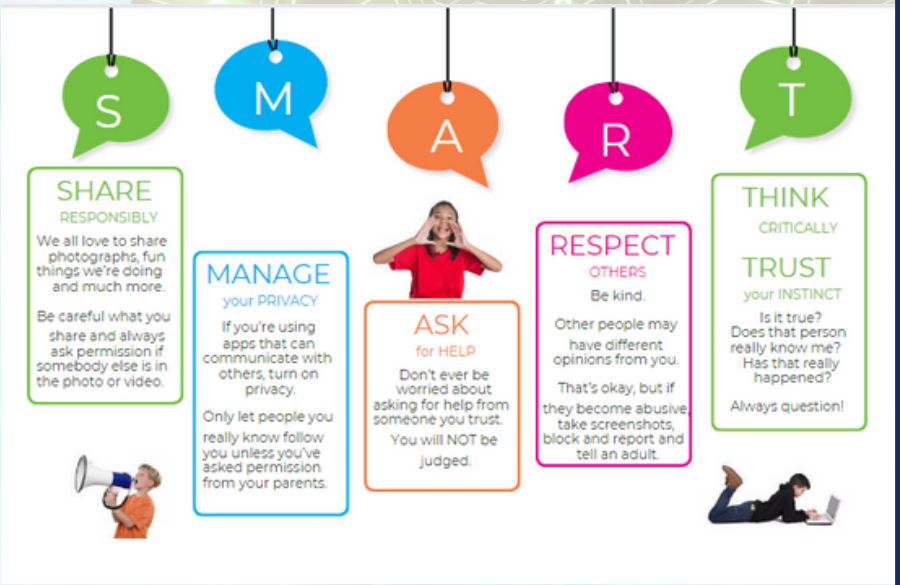
Kids safe online

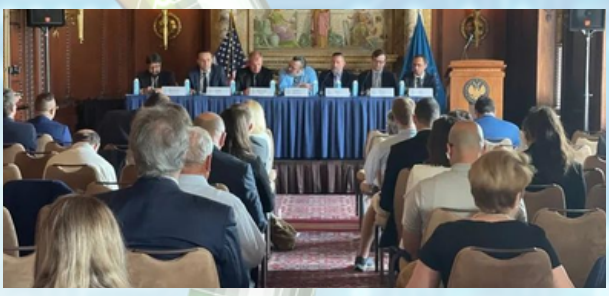
"The internet is a great information tool and can be a place for children to learn, but we need to remember that when children are online, they are in public."

Mark Kennedy

Every day, more than 175,000 children go online for the first time - that's one child every half day.
This digital accessory exposes children to a large number of benefits and opportunities, but also a multitude of risks and harms, to harmful content, sexual abuse and exploitation, cyberbullying and misuse of private information.

The protection of children online as one of the main pillars of the cyber security strategy, is in the constant focus of AKCESK raising constant awareness in Albania to fulfill the full responsibility in forming a safer digital world for children.





Western Balkans: Transatlantic and Regional Cooperation - Building Strong Alliances

On July 13 in Washington, D.C, the Western Balkans Conference: Transatlantic and Regional Cooperation - Building Strong Alliances was organized.
The conference brought together important representatives, with the aim of regional cooperation, which is essential for the countries of the Western Balkans in the progress of the process of stabilizing the association in the EU.
During the session "Cyber Security in the Western Balkans: Meeting the Challenges", Albania, represented by the General Director of AKCESK Mr. Igli Tafa, presented the security challenges recalling the attack of a year ago directed at Albania, in which two main terms were adopted: technological terms where the focus has been the increase of technological capacities as well as strategic terms where the focus has been the raising of human capacities.
Also, following the discussions of this session, the head of AKCESK emphasized the support of strategic partners and the importance of continuous cooperation to deal with critical situations in a stable manner.
The conference continued the discussions by addressing the challenges, ongoing cyber attacks on public and private institutions and individuals and what are the appropriate measures to be taken in strategic terms and international cooperation.

Workshop: "Qeverisja e krizës kibernetike"

In the framework of the development of the capacities of information infrastructures, AKCESK in cooperation with CRDF Global and C3I organized the workshop on "Governance of the cyber crisis".
The purpose of the workshop was to strengthen cross-sectoral cooperation in terms of cybercrisis governance at the national level, through dedicated fictitious scenarios.

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

WEEKLY BULLETIN
10-14 JULY 2023

Quote of the week

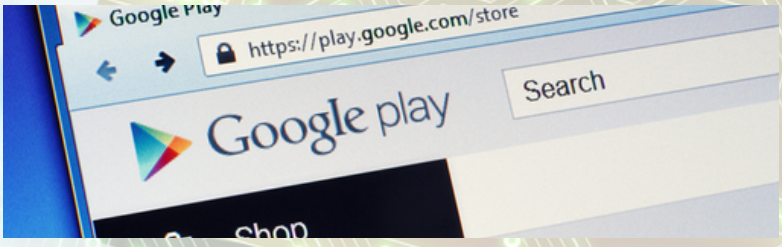
"When functionality is all that matters, security is often overlooked."

Contetn:

CISA gives US civilian agencies until August 1 to fix four Microsoft vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA) has given US federal civilian agencies until August 1 to resolve four serious zero-day vulnerabilities announced as part of Microsoft's monthly Patch Tuesday release.
The inclusion of four vulnerabilities — CVE-2023-32046, CVE-2023-32049, CVE-2023-35311, CVE-2023-36874 — in the CISA catalog means the vulnerabilities are already being exploited by hackers. The four Microsoft vulnerabilities mentioned are among more than 130 announced by the tech giant on Tuesday.
Microsoft confirmed that the vulnerabilities were being exploited and affected all versions of Microsoft Outlook from 2013 onwards.
In addition to Microsoft's announcements, several other companies, including Apple, Google, SAP, Fortinet, Adobe and Cisco, published advisories about their vulnerabilities.

Read more



USB drive malware attacks are on the rise again in the first half of 2023

Researchers have managed to detect two malware campaigns executed via USB; one named "Sogu", attributed to a Chinese espionage threat group "TEMP.HEX" and another named "Snowydrive", attributed to UNC4698, which targets oil and gas firms in Asia.
Most of the casualties belong to the pharmaceutical, IT, energy, communications, healthcare and logistics sectors, but there are casualties across the board.
Sogu is currently the most aggressive USB-assisted cyber espionage campaign, targeting many industries worldwide and attempting to steal data from infected computers.

While USB attacks require physical access to target computers to achieve infection, they have unique advantages that keep them relevant and trending in 2023

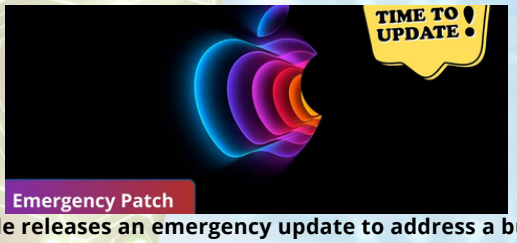
Read more

ING Bank - has confirmed that the information of some of its customers has been accessed by hackers responsible for a series of global attacks using the MOVEit file transfer system

MOVEit is an American company that enables the transmission of data securely between different companies and systems around the world. The attacks were carried out by the cybercriminal group Cl0p, which uses double blackmail methods. By training their victims first to decrypt the data, and then not to publish confidential data.
Unauthorized persons gained access to personal data that the service provider processes in order to switch accounts
ING said that each affected customer will be informed by the bank "in writing" about the incident. The bank's notification will also provide "security instructions" to affected customers to further protect their personal information, as well as "contact options for questions." "The relevant security vulnerability was closed by the service provider and the relevant data protection authorities and law enforcement authorities were informed about the incident.

Read more

PATCHING ALERT



Apple releases an emergency update to address a bug in iOS and macOS

Apple has just released an emergency update to its users to fix the vulnerabilities discovered in the security systems of IOS and MAC.
The vulnerability was discovered in Apple's WebKit browser engine and allows attackers to get arbitrary code execution on target devices by tricking users into opening websites with maliciously crafted information.
IOS and MAC users make the necessary updates as soon as possible and keep the automatic updates option enabled on their devices.

AKCESK recommends all apple users to install the necessary updates

Read more

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