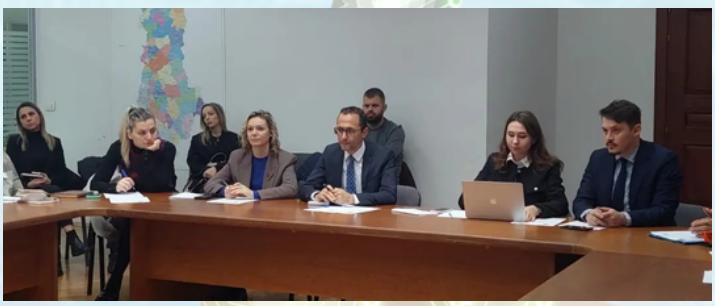
CYBER SECURITY NEWS BULLETIN

December 2023

Content:

- A decade of awareness for children's online safety
- "Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, NAIS and the State Police.



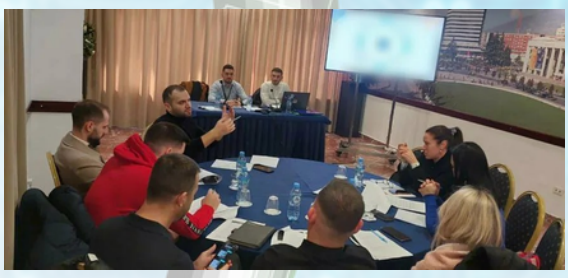
A decade of awareness for children's online safety

The National Authority for Electronic Certification and Cyber Security, focused on the implementation of the strategic policy for increasing the safety of children in cyberspace, organized in cooperation with the international organization International Telecommunication Union (ITU), on December 6, the workshop on the topic "A decade of awareness for children's online safety."

This workshop was carried out as part of the completion of a two-year project initiated from September 2021 to December 2023, where the main goal is to create a safe cyber space for children through capacity building and awareness with numerous trainings and awareness campaigns for three interest groups such as children and young people, teachers, parents and social workers as well as industry sector subjects. During the workshop AKCESK presented the results and activities developed for the implementation of this project throughout the territory of the Republic of Albania.

Participants were state institutions that focus on the protection of children and young people such as MAS, ASHDMF, AKEP, QPKMR, State Police, representatives from Internet Service Providers (ISP), also many non-governmental organizations representing civil society, where during discussions showed their ongoing work in the protection of children, raised issues related to legal gaps and the need for change in the legislation in force, as well as discussed the bridges of cooperation and the creation of ongoing projects in the future through competent institutions, civil society and international partner organizations such as ITU.

In this workshop, the importance of awareness in the field of protecting children online was emphasized, providing resources and tools that support children, parents, teachers, educators, social workers, taking the necessary measures to create a safer online ecosystem.



"Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, NAIS and the State Police.

In continuation of NAECCS objective of increasing capacities as one of the main pillars for the protection of information infrastructures with the support of our partner Risi Albania/Helvetas and the valuable contribution of the Authority's experts, on December 20, 21, 22, was organized the anticipated training on "Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, National Agency of Information Society and the State Police.

For the very importance that these sectors have in terms of the information infrastructures they manage, during this three-day training, presentations were made regarding the legal framework, strategy, policies, the necessary security measures that must be taken by the information infrastructures and the needs for cyber governance.

An important part of this training was the development of three different TTX scenarios for cyber incident management. Also, 2 days of cyber training (Cyber Drill) were held with concrete exercises on cyber incident management, via the FISA.al platform.

In fulfillment of the objectives to achieve international standards in the field of cyber security, NAECCS will continue to organize training for all sectors that administer critical and important information infrastructures in order to build a sustainable cyber ecosystem in Albania.

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

CYBER SECURITY NEWS BULLETIN

December 2023

Content:

- Microsoft warns that hackers are exploiting OAuth applications
- The application which enables scanning of Barcodes on Android, exposes passwords to users
- Toyota - data breach
- Google - patching alert

Microsoft warns that hackers are exploiting OAuth applications

The Microsoft Threat Intelligence team warns that cybercriminal groups are using OAuth applications as an automation tool to deploy virtual machines (VMs) and launch phishing attacks.

To mitigate the risks associated with such attacks, it is recommended that organizations implement multi-factor authentication (MFA), enable conditional access policies, and routinely audit approved applications and permissions.

Read more

Toyota - data breach

Toyota has warned customers that it has suffered a data breach, stating that sensitive personal and financial information was exposed during the attack.

The threat actors demanded a payment of $8,000,000 to delete the stolen data and gave Toyota 10 days to respond to their blackmail.

Toyota promises to update affected customers immediately if the internal investigation reveals further data exposure.

Read more

The application which enables scanning of Barcodes on Android, exposes passwords to users

Security researchers have recently discovered the Barcode to Sheet Android app, which leaks sensitive user and enterprise information stored by the app's creators.

The security team discovered that the app's developers have left their Firebase database, containing over 368 MB of data, open for easy access.

Read more

PATCHING ALERT

Google - patching alert

Google has released an emergency update to address a new zero-day vulnerability, identified as CVE-2023-7024, in the Chrome browser.

The vulnerability has been addressed with the release of version 120.0.6099.129 for Mac, Linux and 120.0.6099.129/130 for Windows, which will be released in the coming days/weeks.

Read more

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