

CYBER SECURITY NEWS BULLETIN



February 2024

Content:

- Conference: “A safer cyber space for children”
- NAECCS in strengthening cyber security capacities



Conference: “A safer cyber space for children”

In the framework of the “International Safe Internet Day”, NAECCS in cooperation with ASHDMF, organized the Conference on “A safer cyberspace for children”. This conference was organized in the premises of the Prime Minister’s Office, in the Center for Openness and Dialogue (COD), on February 6, 2024, where the two heads of institutions, Mr. Igli Tafa and Mrs. Alma Tandili signed the cooperation agreement between the two institutions responsible for meeting the objectives for the protection of children and young people online. The institutions committed to implement a common action plan throughout the year 2024, to carry out various activities and awareness campaigns.

At the Conference, a proactive discussion was held with children and young people invited from two schools in Tirana, the Kosova middle school and the Sami Frashëri High School, on the many risks they face in the digital space, how to protect and report cases of abuse or the distribution of images with inappropriate content, as well as the measures that must be taken by the institutions responsible for raising awareness and protecting children.

At the Conference, Mrs. Bora Muzhaqi Minister of State for Youth and Children, Mrs. Clarisse Pasztory, the Deputy Head of the OSCE Presence in Albania held a speech, as well as representatives from various institutions such as the Embassy of Netherlands, the Swiss Embassy, the State Police, the Municipality of Tirana, Alo 116 111, AKEP, AMA, Risi Albania, the organization Save the Children, etc., who shared their experiences regarding cases where children have been the subject of abuse, bullying or victims of illegal content material distributed online.



NAECCS in strengthening cyber security capacities

In the framework of the creation of a safe cyber ecosystem for business in Albania, on January 31, 2024, the “Cybersecurity Hackathon” activity was organized with participants from the business sector, under the direction of the Albanian Trade Union with the support of NAECCS and the Risi Albania project, implemented by Helvetas.

Considering the digitization of processes and the evolution of technologies that businesses use as well as the increase in the number of cyber security threats, the development of human and technical capacities in this area is essential to guarantee the security and continuity of business operations. This activity, organized in the format of a cyber training, created the opportunity for IT and cyber security experts of businesses to test and expand their knowledge under the guidance of NAECCS professional trainers. The cyber training focused on the implementation and management of simulated cyber attacks, with the aim of developing defensive tactics for the main business systems in Albania.

Deputy Director of NAECCS, Mrs. Floreta Faber, in her welcoming speech, expressed gratitude for the cooperation with RISI Albania in organizing joint activities and emphasized the importance of public-private cooperation for addressing cyber security challenges in the country. The key role of NAECCS was also underlined, to provide continuous support and cooperation to businesses and all critical sectors in Albania, for strengthening cyber security at the national level.

CYBER SECURITY NEWS BULLETIN



February 2024



Albania a Step Closer to Global Cyber Security

NAECCS becomes a member of FIRST

NAECCS's membership in FIRST marks a key moment in the development of Albania's cyber security capacities. The Global Forum of Incident Response and Security Teams (FIRST) is the premier organization and global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents. This agreement makes NAECCS an important part of the global incident response and cyber security community through:

Enhancing international reputation Interaction with the best international expertise in the fight against cyber threats. Access to specialized resources and platforms on new threats, attack techniques, and advanced tools of cyber protection. Active participation in the development of standards and policies.



NAECCS organizes the two-day Cyber Hygiene training

Not updating the operating system, phishing scams or SMishing are a number of risks in today's digital world that can compromise your online security!

This is the reason why NAECCS, in cooperation with CRDF, with the support of the US Department of State, organized the two-day training on Cyber Hygiene on February 12 & 13.

This training was attended by 420 online participants as well as 50 participants in the hall including employees of different profiles from all public institutions, the private sector and civil society. During the training, issues such as keeping the operating system up-to-date, using safe and unique passwords, activating two-factor authentication, and being careful with suspicious links or downloads were addressed.

NAECCS appreciates the involvement of all categories of society in such trainings in order to raise awareness and increase vigilance against ongoing cyber threats.

Content:

- Albania a Step Closer to Global Cyber Security
- NAECCS organizes the two-day Cyber Hygiene training
- Tik Tok - data breach
- Android - patching alert



Tik Tok- data breach

The European Union (EU) is opening a formal investigation into TikTok over potential online content breaches, putting the platform at risk of a significant fine. The investigation will focus on the design of TikTok's system, including algorithmic systems that may stimulate behavioral addictions of the users. The European Commission will also investigate whether TikTok has put in place appropriate measures to ensure a high level of privacy, safety, and security for minors

[Link: Read more](#)

PATCHING ALERT



Android - patching alert

Google released the Android security patch in February 2024 to address 46 vulnerabilities, including a critical remote code execution vulnerability identified as CVE2024-0031. Google released Android security patch level 2024-02-01 and 2024-02-05 to fix the issues found. Users should apply security patches as soon as software updates are available to them.

[Link: Read more](#)