WEEKLY BULLETIN
17-21 JULY 2023

Quote of the week

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Content:

Cyber Security in the Academic Sector

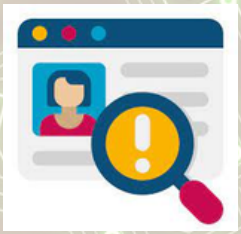
"Students are practically born with technology in their hands, but they don't have enough safety information"

CISO from a major university in Canada

As online learning has become so widespread and offers so many positive opportunities for students and teachers, it is more important than ever to strengthen cybersecurity defenses to deal with new and evolving attacks.

Cyber attackers are constantly discovering new exploits and strategies to compromise users. Here are five best cybersecurity practices for students to help you protect yourself from them:

1. Avoid sharing personal information:
Be careful about the information you disclose online – such as your school name, email address, home address and phone numbers.



2. Invest in virus protection:
Make sure you have antivirus installed on all devices (desktop, laptop, tablet, etc.). Set it to update automatically and run virus scans at least once a week.

3. Keep your software up to date:
Make sure you keep your operating system, and applications fully updated.

4. Be careful about phishing attacks:
Do not open email attachments from illegitimate sources. You may receive emails from group members or teachers, but be careful when opening any attachments.

5. Be careful what you click:
Avoid visiting unknown websites or downloading software from untrusted sources. These sites may contain malware that compromises your computer.

Workshop: "Cyber Defense Strategy Development"

On July 18-21, 2023, the Security Governance Institute of the US Defense Security Cooperation Agency organized the "Cyber Defense Strategy Development" workshop near the premises of the General Staff of the Armed Forces.

Participants in this workshop were representatives from the Ministry of Defense, the General Staff of the Armed Forces, the Military Cyber Security Unit, the National Agency of the Information Society and AKCESK.

The purpose of the workshop was the development and implementation of the cyber defense strategy, to support the mission and harmonize the priorities, structures, decisions and objectives of the Ministry of Defense, for the protection of the Albanian cyberspace.

In the framework of raising the technical capacities of Critical Infrastructures, the National Authority for Electronic Certification and Cyber Security participated in the four-day training developed by USEA and Catalisto together with the assistance of USAID in Tirana.

The focus of the program was the deepening of advanced knowledge in the management of cyber incidents in public and private infrastructures in Albania, as well as the evaluation of the implementation of security measures based on the most recognized international standards.

Active participation in this training serves AKCESK directly in creating sustainable capacities to address potential crises through strengthening strategies, innovation and cyber security.

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

Autoriteti Kombëtar për CESK

autoriteti_kombetar_cesk

+35542221039

WEEKLY BULLETIN
17-21 JULY 2023

Quote of the week

"Të argumentosh se nuk të intereson e drejta e privatësisë sepse nuk ke asgjë për të fshehur nuk është ndryshe nga të thuash se nuk të intereson liria e fjalës sepse nuk ke çfarë të thuash."

Content:

Microsoft: Hackers turn Exchange servers into malware control centers

Microsoft warns of new attacks by the Russian state-sponsored hacker group Turla, which are targeting the defense industry and Microsoft Exchange servers using a new 'DeliveryCheck' malware backdoor.
Attacks start with phishing emails that contain EXEL documents attached containing malicious macros. When activated, these macros run a PowerShell command, thereby creating a flow of scheduled tasks that mimic the Firefox browser.
This malware is a cyber espionage tool that allows threat actors to execute javascript on devices, steal data from event logs, steal information about system files, and steal credentials from a variety of programs, including browsers, clients FTP, VPN software, KeePasok, Outlook, Az, and Azure.

Read more

GitHub warns of Lazarus hackers

GitHub warns of an attack campaign that uses social engineering and targets developer accounts in the blockchain, cryptocurrency, online gambling and cybersecurity sectors to infect their devices with malware.
According to GitHub Lazarus Group is compromising legitimate accounts or creating fake personas pretending to be developers and recruiters on GitHub and social media.
Once victims trust them, threat actors invite them to collaborate on a project during which they download malware to victims' devices.

A similar campaign was carried out in March 2021 where hackers created a website for a fake company called SecuriElite and used it to infect victims' devices with malware

Read more

VirusTotal exposes some details of registered customers

Data associated with a subset of registered VirusTotal customers, including their names and email addresses, was exposed after an employee unwittingly uploaded the information to the malware scanning platform.

Launched in 2004, VirusTotal is a popular service that analyzes suspicious files and URLs to detect types of malware and malicious content using antivirus engines and website scanners.

VirusTotal apologized for the latest customer data exposure incident, stating that it was caused by an employee who accidentally uploaded a CSV file to the platform on June 29, 2023, containing information about his Premium account customers. especially their names, and email addresses of group administrators.

Read more

PATCHING ALERT

Oracle releases 508 new security updates

Oracle recently published 508 security patching alerts in which more than 350 address vulnerabilities that can be exploited remotely without authentication. Some of these vulnerabilities affect multiple products.
The tech giant also released the July 2023 Solaris bulletin, which includes 17 security patches, including 11 for vulnerabilities that are remotely exploited, and also announced the release of 42 security patches as part of its July 2023 Linux bulletin.

Customers are advised to apply available patches in a timely manner, or block network access to unpatched applications, to reduce the risk of an attack.

Read more

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