



AKCESK

**AUTORITETI KOMBËTAR PËR
CERTIFIKIMIN ELEKTRONIK
DHE SIGURINË KIBERNETIKE**

Raport për aktivitetet e vitit 2020

Rr. "Papa Gjon Pali II", Nr. 3, Kati I
Tiranë, Shqipëri

Përmbajtja

I. Aktivitete ndërgjegjësuese.....	3
“Dita Ndërkombëtare e Internetit të Sigurt 2020” #CyberCorner	3
Tetori – Muaji European i Ndërgjegjësimit për Sigurinë Kibernetike	4
II. Aktivitete për ngritjen e kapaciteteve.....	5
CyberSec 1.0.....	5
Albanian Cyber Academy 4 (ACA4).....	5
Cybersec 2.0.....	6
III. Materiale promovuese.....	7
Postera.....	7
Video.....	9
IV. Rekomandime për Sigurinë në Internet (Situata Covid-19)	12

Gjatë vitit 2020, me qëllim të përmbushjes së detyrave funksionale ka realizuar aktivitete të ndryshme ndërgjegjësuere dhe aktivitete për rritjen e kapaciteteve të ekipeve të CSIRT sektorial dhe CSIRT kombëtar.

AKCESK në cilësinë e CSIRT kombëtar është anëtar i akredituar në Trusted Introducer nga 27 Maj 2020 dhe “*Fellow Member*” në FIRST (Forum for Incident Response Teams) 24 Shkurt 2020.

Aktivitete të tjera janë:

I. Aktivitete ndërgjegjësuere

“Dita Ndërkombëtare e Internetit të Sigurt 2020” #CyberCorner

Në kuadër të Ditës Ndërkombëtare të Internetit të Sigurt Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) në bashkëpunim me Bashkinë Tiranë dhe me mbështetjen e Raiffeisen Bank dhe Telekom Albania, lançuan projektin inovativ #CyberCorner në bibliotekën “Hamit Beqja”, pranë Njesisë Administrative Nr.8, Tiranë.

Projekti synon rritjen e ndërgjegjësimit për sigurinë e fëmijëve në Internet dhe aftësimi i tyre për përdorimin e e-shërbimeve në ambientet tashmë multifunksionale të bibliotekës “Hamit Beqja”. CyberCorner do të ofrojë për fëmijët dhe të rinjtë mundësi për njohuri të thelluara mbi tematikat aktuale dhe sensitive, si: përdorimi i internetit të sigurt, kodimi, radikalizmi dhe ekstremizmi i dhunshëm, shërbimet elektronike publike. Për secilën nga këto tema janë hartuar module, si dhe janë instaluar pajisje kompjuterike, me të cilat mund të ndërveprohet gjatë qëndrimit në ambientet e bibliotekës dhe do të organizohen nëpërmjet workshopeve nga ekspertët e AKCESK.





Tetori – Muaji Europian i Ndërgjegjësimit për Sigurinë Kibernetike



AKCESK gjatë muajit tetor ka realizuar fushata ndërgjegjësimi me nxënësit e shkollave nëntëvjeçare dhe të mesme të kryeqytetit me qëllim “Rritjen e nivelit të sigurisë së fëmijëve dhe të rinjve në internet”. DCAF në bashkëpunim me AKCESK, UK Government dhe British Embassy në Tiranë kanë realizuar një seri videosh në gjuhën shqipe rreth Back up Data, CEO Frauds, Online Scams and Passwords për ta bërë më të kuptueshme rëndësinë e sigurisë kibernetike, nën moton "Jeta nuk është një përrallë".

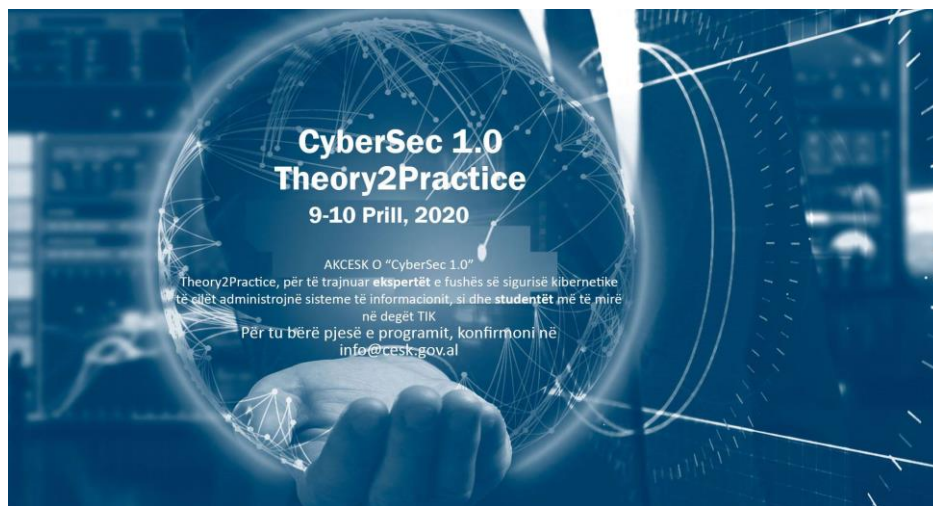
Foto nga aktiviteti me nxënësit e shkollave:



II. Aktivitete për ngritjen e kapaciteteve

CyberSec 1.0

AKCESK, në cilësinë e Autoritetit përgjegjës për sigurinë kibernetike në Republikën e Shqipërisë organizoi trajnimin online “CyberSec 1.0”, për rritjen e kapaciteteve të stafit përgjegjës të CSIRT-eve sektoriale dhe studentet e TIK. Trajnimi dy-ditor siguroi një pjesëmarrje prej 35 pjesëmarrësish unikë në ditë.



Albanian Cyber Academy 4 (ACA4)

Albanian Cyber Academy

4-th Edition

22 June - 3 July 2020



17

11 International speakers,
6 local experts



600+

participants in 2 weeks,
65% women



2

hands on sessions
conducted

Edicioni i 4 i Akademisë së Sigurisë Kibernetike u organizua në datat 22 Qershor - 3 Korrik.

Qëllimi i këtij aktiviteti ishte rritja e kapacitetit dhe thellimi i njohurive të profesionistëve të sigurisë kibernetike dhe studentëve të rinj të talentuar të fushës.

Gjatë ACA4 morën pjesë 11 ekspertë ndërkombëtarë dhe 6 ekspertë vendas, nga të cilët mund të përmendim Dr. Erdal Ozkaya, Mitko Bogdanoski, Ramsés Gallego, Ljubica Pendaroska, Ivica Simonovski, Elio Pashaj, Predrag

Pale, Metodi Hadji Janev, Marjan Stoilkovski, Ogerta Elezaj, Eralda Dharmo (Gjika), Elda Kuka, të cilët ndanë ekspertizën e tyre me mbi 600 pjesëmarrës online dhe më shumë se 60 pjesëmarrës unikë në ditë.

Cybersec 2.0

AKCESK, në cilësinë e Autoritetit përgjegjës për sigurinë kibernetike në Republikën e Shqipërisë organizoi trajnimin online "**CyberSec 2.0**" në datat 17-18 Dhjetor 2020. Aktiviteti synoi rritjen e kapaciteteve dhe thellimin e njohurive në fushën e sigurisë kibernetike të operatorëve të infrastrukturave kritike të informacionit, si dhe promovimin e bashkëpunimit për ofrimin e trajnimeve specifike mbi "**MDFIR Certified DFIR Specialist certification**" dhe "**MTIA - Certified Threat Intelligence Analyst**" për anëtarët e CSIRTs sectorial në bashkëpunim me **Mosse Cyber Security Institute**.

Në kuadër të ngritjes së kapaciteteve është bërë e mundur :

1. Pjesëmarrja në webinarë të organizuar nga Këshilli i Europës, OSCE, dhe Carnegie Mellon University me tema:
 - a) Kripto për Autoritetet e Drejtësisë Penale,
 - b) Grupi i Punës i Ballkanit Perëndimor,
 - c) Ligjet Ndërkombëtare të Operacioneve Kibernetike.
2. Pjesëmarrja në:
 - a) SANS Institute : Reverse Engineering Malware – Malware Analysis Tools and Techniques

b) Carnegie Mellon - Western Balkans Working Group, Steps for Creating National CSIRT

III. Materiale promovuese

Përgjatë vitit 2020 në zbatim të planit të komunikimit të sektorit u realizua publikimi periodik i **4 posterave** dhe **8 videove promovuese** për ndërgjegjësimin e komunitetit për rritjen e nivelit të sigurisë kibernetike të realizuara me mbështetjen e DCAF.

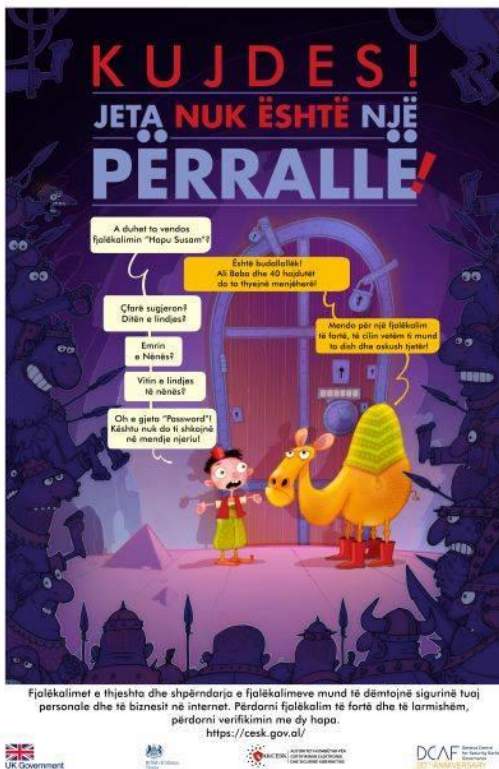
Postera



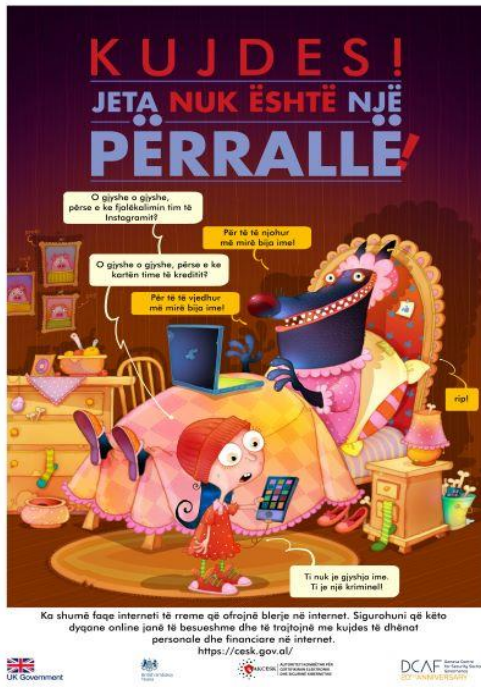
1. "Grupet kriminale shpesh përdorin malware për shantazh ndaj bizneseve që nuk kanë aftësi mbrojtjeje aktive në internet. Si një mbrojtjeje e mundshme bëni një kopje rezervë të informacionit kritik të biznesit në mënyrë periodike"



2. Bizneset dhe sektori bankar shpesh janë nën këto lloj kërcënimesh. Verifikoni besueshmërinë e dërguesit të postës elektronike dhe trajtoni me kujdes të dhënat e kompanisë në internet.



3. “Fjalëkalimet e thjeshta dhe shpërndarja e fjalëkalimeve mund të dëmtojnë sigurinë tuaj personale dhe të biznesit në internet. Përdorni fjalëkalim të fortë dhe të larmishëm, përdorni verifikimin me dy hapa”



4. "Ka shumë faqe interneti të rreme që ofrojnë blerje në internet. Sigurohuni që këto dyqane online janë të besueshme dhe të trajtojnë me kujdes të dhënat personale dhe financiare në internet"

Video

👉 Si të krijoni një password të sigurt 🛡️

<https://www.youtube.com/watch?v=kxRMEys3sJA&feature=youtu.be>



YOUTUBE.COM
Passwords

👉 Kujdes! Jeta nuk eshte nje perralle!

<https://www.youtube.com/watch?v=Y5BAbuMEAh0&feature=youtu.be>



YOUTUBE.COM
Online scam

👉 Always doublecheck first 🤔😭 !! ✅

#AKCESK #DCAF

<https://www.youtube.com/watch?v=9AeFgaqZDZo&feature=youtu.be>



YOUTUBE.COM
CEO frauds

👉 !! Sa e rëndësishme është të keni kopje rezervë të të dhënave tuaja ose të biznesit tuaj ? 😭

AKCESK në bashkëpunim me DCAF kanë përgatitur për ju një video sensibilizuese. #AKCESK #DCAF #BACKUP

👉👉👉

<https://www.youtube.com/watch?v=PYU8Fp5h54s&feature=youtu.be>



YOUTUBE.COM
Back up data
Rëndësia e back up

Gjithashtu AKCESK ka realizuar **4 video** mbi: **Cyber Health, Online Safety, Cyber Hygiene, Cyberbullying**. Materialet mund të gjenden në kanalin zyrtar të Autoritetit në YouTube. Në kuadër të muajit Evropian të Sigurisë Kibernetike dhe edukimit të klientit bankar, AAB ka organizuar tre Webinars. Programi u përqendrua në tema që ndihmojnë njerëzit të identifikojnë dhe të përgatiten për kërcënimet kibernetike. Fushatat vënë theksin në disa hapa të thjeshtë të cilët mbrojnë të dhënat tona personale, profesionale dhe financiare.

👉 Edukohu cyber !!

#thinkcyber #akcesk... See More

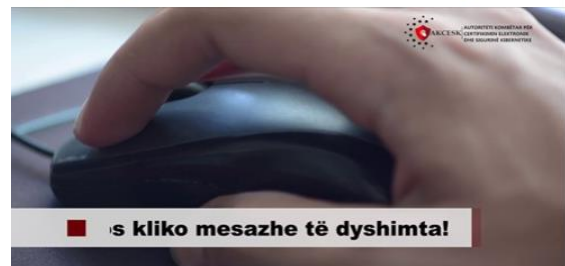


YOUTUBE.COM
Cyber health

👉 APLIKO Cyber Hygiene !!

✅

<https://www.youtube.com/watch?v=Nb-sNKGxrGI&feature=youtu.be>



YOUTUBE.COM
Cyber hygiene

👉 Nëse ndiheni të frikësuar për sigurinë tuaj online 👤👤, kërkonti ndihmë! ✅ . #aksesk #dcaf #onlinesafety

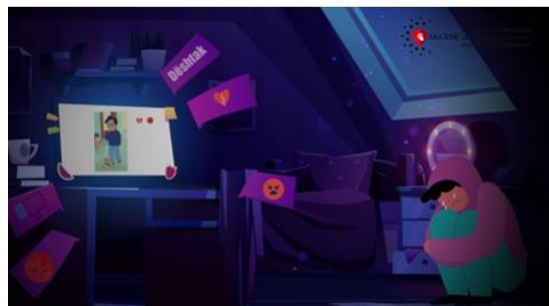
<https://www.youtube.com/watch?v=517ephhHAJE&feature=youtu.be>



YOUTUBE.COM
Online safety

👉 Injoro mesazhet kërcënuese ose tallese!

<https://www.youtube.com/watch?v=0UkEJdwMIEY&feature=youtu.be>



YOUTUBE.COM
Cyberbullying

Gjithashtu, është organizuar seria e trajnimeve online për prindërit dhe edukatorët me temë "*Siguria e fëmijëve në Internet*" me mbështetjen e ITU. Trajnimet u organizuan online për pesë ditë, nga **15-19 nëntor 2020**. Synimi i këtij trajnimi ishte inkurajimi i një sjelljeje më të sigurt në Internet për fëmijët dhe të rinjtë, duke theksuar këshillat për prindërit dhe edukatorët në komunikimin, suportin dhe edukimin ndaj tyre. Me rreth **100 pjesëmarrës unikë** brenda dhe jashtë Shqipërisë, të cilët shfaqën interesin, entuziasmin dhe rëndësinë e rritjes së njohurive në tema të tilla, ky event arriti suksesin e tij duke motivuar dhe qenë një nxitje e vijimësisë së trajnimeve të ngjashme në fushën e TIK e jo vetëm.

Roli që luajnë prindërit dhe mësuesit

Prindërit duhet të kenë qasjen e duhur ndaj një fenomeni të tillë dhe të jenë mbështetja kryesore për fëmijët e tyre.

Fushat që prindërit dhe mësuesit duhet të konsiderojnë janë:

- ❖ Siguria dhe privatesia e teknologjive
- ❖ Edukimi i prindërve dhe kujdestarëve rreth problematikave të fëmijëve në Internet
- ❖ Rishikimi i karakteristikave të faqeve të Internetit
- ❖ Edukimi i fëmijëve

IV. Rekomandime për Sigurinë në Internet (Situata Covid-19)

Duke bashkëpunuar me partnerë ndërkombëtarë si: Qualys, EATM Cert, Shadowserver dhe me sektorët e tjerë të AKCESK (sektori i Kontrollit) janë prodhuar dhe publikuar në interval kohor (javor dhe 2-javor) të rekomandimeve si dhe vulnerabiliteteve të evidentuara të sistemeve TIK. Këto raporte përditësimi u janë dërguar OIKI dhe OIRI me anë të Sistemit të Monitorimit dhe Menaxhimit të Incidenteve si dhe nëpërmjet e-mailit zyrtar të institucionit për ata operatorë të cilët kanë hasur problem në aksesimin e sistemit.

- Rekomandime për Sigurinë në Internet kur Punoni nga Shtëpia për Punëdhënësit dhe Stafin
- Rekomandime për Sigurinë në Internet për Blerje Shitje Online për Qytetaret dhe Bizneset
- Rekomandime dhe Këshilla për Përdorimin e platformës ZOOM
- Rekomandime mbi Sulmet Phishing
- Njoftime mbi Sigurinë/ Security Update
- Rekomandimi për Kujdes nga kriminelët që pretendojnë të jenë WHO
- Vulnerability Alert - Adobe ka lëshuar 21 "Patche" kritike në Illustrator dhe Bridge
- Vulnerabilitet "zero day" në IOS
- CVE-2020-0796 SMBv3 Vulnerability
- Betternet & PrivateVPN
- Vulnerabilitet në Microsoft Teams
- Vulnerabilitete në librarinë Autodesk FBX në Word dhe Office
- Tre vulnerabilitete kritike në Mozilla Firefox
- Produktet Sophos XG Firewall, viktime të një sulmi zero-day
- Vulnerabilitet XSS në VMware ESXI