BULETINI JAVOR
4-8 DHJETOR 2023

Shprehja e javës

"Siguria është gjithmonë e tepruar derisa nuk mjafton."

Robbie Sinclair

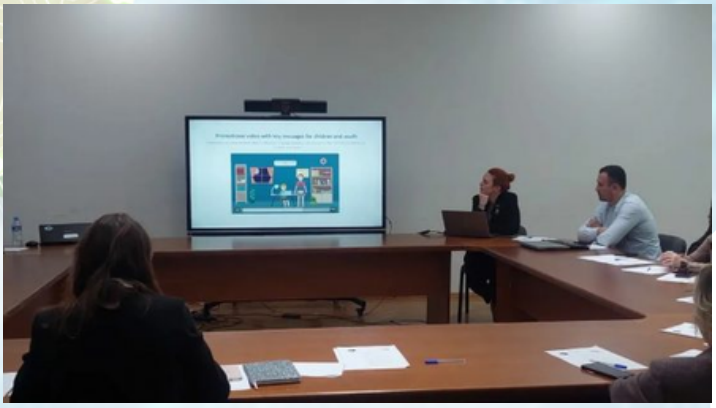
Përmbajtja:

Një dekadë ndërgjegjësim për sigurinë online të fëmijëve

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike fokusuar në implementim e politikës strategjike për rritjen e sigurisë së fëmijëve në hapësirën kibernetike, organizoi në bashkëpunim me organizatën ndërkombëtare International Telecommunication Union (ITU), datën 6 dhjetor workshop-in me temë "Një dekadë ndërgjegjësim për sigurinë online të fëmijëve."

Ky workshop u realizua në kuadër të përmbylljes së një projekti dy vjeçar iniciuar në shtator 2021 deri në dhjetor 2023, ku qëllimi kryesor është krijimi i një hapësirë kibernetike të sigurt për fëmijët përmes rritjes së kapaciteteve dhe ndërgjegjësimit me trajnime të shumta dhe fushatave ndërgjegjesuese për tre grupe interesi si fëmijët dhe të rinjtë, mësuesit, prindërit dhe punonjësit social si dhe subjekte të sektorit të industrisë. Gjatë workshop-it AKCESK prezantoi rezultatet e aktivitetet e zhvilluara për implementimin e këtij projekti në të gjithë territorin e Republikës së Shqipërisë.

Pjesëmarrës ishin institucione shtetërore që kanë në fokus mbrojtjen e fëmijëve dhe të rinjve si MAS, ASHDMF, AKEP, QPKMR, Policia e Shtetit, përfaqësues nga Ofruesit e Shërbimit të Internetit (ISP), gjithashtu dhe shumë organizata joqeveritare përfaqësues të shoqërisë civile, ku gjatë diskutimeve treguan punën e tyre të vazhdueshme në mbrojtje të fëmijëve, ngritën problematika në lidhje me boshllëqet ligjore dhe nevojën e legjislacionit në fuqi për ndryshim, si dhe u diskutua mbi urat e bashkëpunimit dhe krijimin e projekteve vazhdueshme në të ardhmen nëpërmjet institucione kompetente, shoqërisë civile dhe organizatave ndërkombëtare partner si ITU.



Në këtë workshop u theksua rëndësia e ndërgjegjësimit në fushën e mbrojtjes së fëmijëve në internet, duke ofruar burime dhe mjete që mbështesin fëmijët, prindërit, mësuesit, edukatorët, punonjësit social, duke ndërmarrë masat e nevojshme për krijimin e një ekosistemi sa më të sigurt online.

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

BULETINI JAVOR
4-8 DHJETOR 2023

Shprehja e javës

"Siguria është gjithmonë e tepruar derisa nuk mjafton."

Robbie Sinclair

Përmbajtja:

- **Vulnerabiliteti i ri i Bluetooth i lejon hakerët të sulmojnë pajisjet Android, Linux, macOS dhe iOS**
- **HTC Global Services - data breach**
- **Apliakcioni i cili mundëson skanimin e Barkodeve në Android, ekspozon fjalëkalimet e përdoruesve**
- **Wordpress - patching alert**

Vulnerabiliteti i ri i Bluetooth i lejon hakerët të sulmojnë pajisjet Android, Linux, macOS dhe iOS

Një vulnerabilitet sigurie në Bluetooth mund të shfrytëzohet nga aktorët e kërcënimit për të marrë kontrollin e pajisjeve Android, Linux, macOS dhe iOS.

E identifikuar si CVE-2023-45866, vulnerabiliteti lejon anashkalimin e autentifikimit duke u mundësuar sulmuesve të lidhen me pajisje të ndjeshme për të arritur ekzekutimin e kodit .

[Lexo më shumë]

HTC Global Services - data breach

Kompania e shërbimeve të IT dhe konsulencës së biznesit HTC Global Services ka konfirmuar së fundmi se kanë pasur një sulm kibernetik nga banda e ransomware ALPHV.

Të dhënat e zbuluara përfshijnë pasaporta, lista kontakti, email dhe dokumente konfidenciale që dyshohet se janë vjedhur gjatë sulmit.

[Link: Lexo më shumë]

Apliakcioni i cili mundëson skanimin e Barkodeve në Android, ekspozon fjalëkalimet e përdoruesve

Studiuesit e sigurisë kanë zbuluar së fundmi aplikacionin ***Android Barcode to Sheet,*** i cili rrjedh informacione të ndjeshme të përdoruesit dhe të ndërmarrjeve të ruajtura nga krijuesit e aplikacionit.

Ekipi i sigurisë zbuloi se zhvilluesit e aplikacionit kanë lënë bazën e të dhënave të tyre Firebase, që përmban mbi 368 MB të dhëna, të hapura për t'u aksesuar lehtësisht.

[Link: Lexo më shumë]

PATCHING ALERT

Wordpress-patching alert

WordPress ka publikuar versionin 6.4.2 me një patch për një vulnerabilitet kritik, i cili mund të shfrytëzohet nga aktorët e kërcënimit për të ekzekutuar kodin arbitrar PHP në faqet e cënueshme.
Rekomandohet që përdoruesit të kontrollojnë manualisht faqet e tyre për t'u siguruar që është përditësuar në versionin më të fundit.

[Link: Lexo më shumë]

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