

Ky dokument nuk është prova. Prova janë bajtët e ruajtur: HTML-ja e faqes, pamja e saj, dhe zinxhiri i hash-eve që i lidh. Kjo dëshmi është paraqitja e tyre, e prodhuar automatikisht. Verifikohet me kodin më poshtë **pa na pyetur ne**.

ARTIKULLI

TITULLI	Këshillat/ Si të mbroheni nga kamerat e fshehta
ADRESA	https://lapsi.al/keshillat-si-te-mbroheni-nga-kamerat-e-fshehta-i1094921
BURIMI	lapsi.al
GJENDJA	online

KOHA

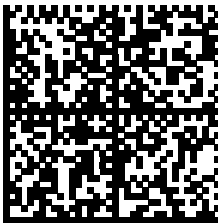
KAPUR NGA NE	2 tetor 2026, 12:09:03 UTC <i>Dritarja jonë e pasigurisë: ± 300 s — intervali me të cilin e kontrollojmë këtë burim.</i>
DEKLARUAR NGA PORTALI	2 tetor 2026, 12:06:00 UTC <i>Koha e deklaruar vjen nga pala që po vlerësohet. Ora jonë nuk preket prej saj, dhe të dyja shfaqen këtu të ndara.</i>

HASH-ET · SHA-256

PËRMBAJTJA	de0a615252271903bb6f06b76c252ecbf2ae8d79ac7d486104b4eafd58ce6428
TEKSTI	d152939ea016fbd99eafca12fa12d9cd2c5c645b7c7fb5379d2c8b4fb7b99034
PAMJA	36649de45b352e16b72fa18af0323d172c523f5e321b1582b3812c7908658608

ZINXHIRI I PROVËS

KJO HYRJE	7ae8fe330db82104f141b9fe71f42cfb1d9e8d5e4a0101daf2b827435b852878
E MËPARSHMJA	—
RRËNJA MERKLE	—
ANKORIMI	nuk është ankoruar ende <i>Kjo hyrje nuk është përfshirë ende në asnjë pemë Merkle të dërguar. Zinxhiri i hash-eve provon rendin dhe integritetin; koha jo.</i>



SKANOJE PËR TA VERIFIKUAR

Kodi të nxjerr te eksploruesi i STAMLES. Ai regjistër nuk është yni: nëse serveri ynë bie nesër, vula mbetet aty ku është.

Faqja tregon njërin nga tri gjendjet — **nuk u gjet**, **në radhë**, ose **e konfirmuar** me bllokun, rrënjën Merkle dhe transaksionin në Polygon. Krahazo hash-in që gjen atje me atë të shtypur më lart: nëse përputhen, kjo kapje ekzistonte para asaj ore, dhe ne nuk mund ta kishim ndryshuar pas saj.

<https://scan.stamles.eu/verify/7ae8fe330db82104f141b9fe71f42cfb1d9e8d5e4a0101daf2b827435b852878>

PAMJA E FAQES

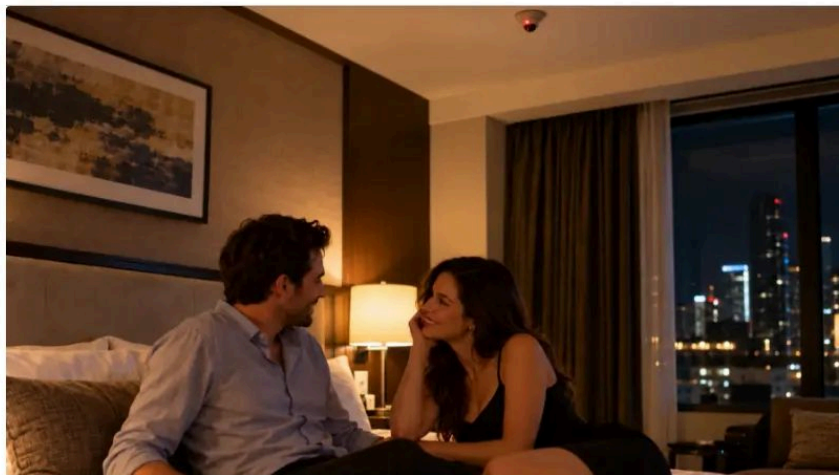
Renderuar nga HTML-ja jonë e ruajtur, jo nga rrjeti. **Riprodhon kopjen tonë, jo pamjen e atëhershme:** stilet dhe imazhet e largëta mund të mos ekzistojnë më ose të kenë ndryshuar.

Motori: chromium-stored+assets · dritarja 1280×1024 px

Këshillat/ Si të mbroheni nga kamerat e fshehta



LAPSI.AL • 2 OCTOBER 2026



Kamerat moderne mund të jenë shumë të vogla, të lidhen me internetin dhe të transmetojnë pamje e zë nga distanca. Disa regjistrojnë edhe pa Wi-Fi, ndërsa të tjera bëhen rrezik serioz nëse kanë fjalëkalime të dobëta, konfigurime të pasigurta ose bien në duar të paautorizuara. Rreziku lidhet edhe me pajisje që regjistrojnë vetëm zë, pa lente të dukshme.

Kamerat e vogla dhe pajisjet inteligjente janë bërë shumë më të qasshme. Shumë prej tyre kontrollohen përmes telefonit, mund të transmetojnë drejtpërdrejt dhe t'i ruajnë regjistrimet në cloud ose në kartë memorie.

Prandaj mbrojtja e privatësisë nuk kufizohet vetëm te kërkimi i një lenteje të fshehur. Duhet të dimë edhe nëse pajisja mund të regjistrojë zë, nëse transmeton nga larg, ku ruhen regjistrimet dhe sa e sigurt është vetë pajisja ose llogaria që e kontrollojnë.

Filloni me një kontroll të thjeshtë të hapësirës

Në hotel, apartament me qira, dhomë gjumi, banjë, dush apo kabinë zhveshjeje, kontrolli i parë duhet të jetë vizual.

Shikoni sidomos objektet që kanë pamje të drejtpërdrejtë drejt shtratit, dushit ose zonës ku ndërrohen rrobat. Vëmendjen duhet ta tërheqin vrimat e pazakonta, sipërfaqet shumë të vogla e të errëta prej xhami, pajisjet e orientuara çuditshëm ose objektet elektronike që nuk duket se kanë arsye të jenë aty.

Kjo nuk do të thotë se çdo detektor tymi, karikues, orë apo pajisje elektronike fsheh kamerë. Një element i pazakontë është vetëm arsye për kontroll më të kujdesshëm, jo provë se po regjistroheni, transmeton Telegrafi.

Fikni dritat dhe kërkoni reflektimin e lentes

Lentet e kamerave mund të reflektojnë dritën. Në një ambient të errësuar, drita e

ide



Ana pozitive e ankthit prej të pandehuri të Edi Ramës
Andi Bushati



Një histori korruptimi jo dashurimi
Blendi Kajsia

MOTITIRANA

26°C

KËMBIMIEURO

92.03

aktuale

07:28

Katër muaj protestë dhe asnjë hap pas, qytetarët dalin sërish kundër qeverisë

21:39



PAMJET/ Përplasje mes protestuesve dhe policisë së Tiranës



Ekosistemi shqiptar i inovacionit prezantohet në Bits & Pretzels: 17 startupe, nga Shqipëria, Kosova dhe diaspora

Ndëqe Lapsin edhe në



Me interes nga publiku



telefonit mund të drejtohet ngadalë drejt objekteve të dyshimta.

Një reflektim i vogël dhe relativisht i fortë mund të jetë indicie se aty ndodhet një sipërfaqe optike. Por kjo metodë nuk është e pagabueshme: xhami, plastika dhe metali gjithashtu reflektojnë dritën, ndërsa një lente e vendosur thellë ose në kënd tjetër mund të mos jetë e dukshme.

Telefoni mund të ndihmojë për kamerat me infra të kuqe

Disa kamera përdorin LED infra të kuqe për të regjistruar në errësirë. Syri i njeriut nuk i sheh këto rreze, por disa kamera telefonash mund t'i perceptojnë.

Një provë e thjeshtë mund të bëhet me telekomandën e televizorit: drejtojeni nga kamera e telefonit dhe shtypni një buton. Nëse në ekran shfaqet dritë e bardhë, rozë ose vjollcë, ajo kamerë mund të perceptojë të paktën një pjesë të rrezatimit infra të kuq.

Më pas, në një dhomë të errësuar, mund të kontrolloni përmes kamerës së telefonit nëse shfaqen pika të vogla të ndritshme pranë një pajisjeje të dyshimtë.

Megjithatë, shumë telefona modernë filtojnë infra të kuqen, ndërsa shumë kamera të fshehta nuk përdorin fare ndriçim infra të kuq. Pra, nëse nuk shihni asgjë, kjo nuk dëshmon se kamera nuk ekziston.

A tregon drita e kuqe se kamera po regjistron?

Jo domosdoshmërisht.

Disa kamera kanë LED që ndizet gjatë regjistrimit, transmetimit ose lidhjes me rrjetin. Te të tjera kjo dritë mund të çaktivizohet ose mund të mos ekzistojë fare.

Prandaj mungesa e një drite të kuqe, blu apo të gjelbër nuk do të thotë se kamera është e fikur. Një pajisje mund të regjistrojë pa zhurmë dhe pa sinjale të dukshme.

Pamjet dhe zëri mund të merren edhe nga larg

Kamerat inteligjente zakonisht lidhen me internetin përmes Wi-Fi-së. Sipas National Cyber Security Centre (NCSC) të Britanisë, kjo u mundëson përdoruesve të shohin transmetimin drejtpërdrejt dhe të marrin njoftime edhe kur ndodhen jashtë shtëpisë.

Por Wi-Fi nuk është mënyra e vetme. Një kamerë mund t'i ruajë pamjet në kartë microSD pa qenë fare e lidhur me internetin, mund të përdorë rrjet celular ose të lidhet me një regjistruar lokal.

Pra, mungesa e Wi-Fi-së nuk do të thotë se pajisja nuk po regjistron.

Jo vetëm pamje – mund të regjistrohet edhe zëri

Shumë kamera moderne kanë mikrofoni të integruar. Federal Trade Commission (FTC) sqaron se kamerat smart dhe IP mund të transmetojnë jo vetëm video, por edhe audio, të cilën përdoruesi mund ta dëgjojë nga telefoni ose kompjuteri.

Ekzistojnë gjithashtu pajisje që nuk kanë fare lente dhe funksionojnë vetëm si regjistruar zëri. Kjo është arsyeja pse një kontroll i privatësisë nuk duhet të kufizohet vetëm te kërkimi i kamerave.

Si mund të ndodhë qasja e paautorizuar nga larg

Qasja nga larg nuk kërkon që personi të jetë fizikisht pranë kamerës.

Nëse një kamerë është e lidhur me internetin, dikush që fiton qasje të paautorizuar në llogarinë, aplikacionin ose rrjetin e saj mund të shohë transmetimin apo regjistrimet dhe, kur pajisja e mbështet, edhe të dëgjojë audion.



Rama nxjerr foton me Trump: U detyrova ta bëj me "IA"



Shpallet projekti fitues, kjo është kulla që do të ngrihet në Parkun Rinia



Agron Shehaj fiton në Apelin e GJKKO-së gjyqin me Adriatik Lapaj



Shkoi të inaguronte kardiokirurgjinë e re, kryeministri Rama pritet me protesta

NCSC paralajmëron se transmetimet ose pamjet e kamerave smart mund, në raste të caktuara, të bëhen të qasshme për persona të paautorizuar. Një rrezik i njohur janë fjalëkalimet e parazgjedhura nga prodhuesi ose fjalëkalimet e dobëta që mund të hamendësohen.

Rrezikun mund ta shtojnë përdorimi i të njëjtit fjalëkalim në disa shërbime, mungesa e verifikimit me dy faktorë, firmware-i i vjetër, aplikacionet e papërditësuara ose komprometimi i telefonit apo kompjuterit nga i cili menaxhohet kamera.

FTC rekomandon përdorimin e fjalëkalimeve unike, aktivizimin e autentikimit me dy faktorë kur ofrohet, si dhe përditësimin e kamerës dhe aplikacionit.

Edhe routeri mund të jetë pika e dobët

Siguria e kamerës lidhet edhe me sigurinë e rrjetit.

NCSC paralajmëron se funksione të routerit si UPnP dhe port forwarding mund, në konfigurime të caktuara, të ekspozojnë pajisjet e rrjetit ndaj internetit dhe rekomandon çaktivizimin e tyre kur nuk nevojiten. Po ashtu këshillon që qasja nga larg të çaktivizohet nëse përdoruesit nuk u duhet.

Për mbrojtje, përdorni fjalëkalime të gjata dhe unike, aktivizoni verifikimin me dy hapa, përditësoni firmware-in e kamerës dhe routerit dhe mos lini të aktivizuara funksione që nuk i përdorni. NCSC gjithashtu këshillon shmangien e pajisjeve që nuk mbështeten më me përditësime sigurie.

A mund ta zbulojë Wi-Fi-ja një kamerë të fshehtë?

Nëse keni qasje të ligjshme në rrjetin Wi-Fi, lista e pajisjeve të lidhura mund të tregojë një pajisje që nuk e njihni.

Por kjo nuk është provë përfundimtare. Kamera mund të regjistrojë vetëm lokalisht, të jetë në një rrjet tjetër ose të paraqitet me një emër teknik që nuk tregon se është kamerë.

Prandaj aplikacionet që premtojnë se “zbulojnë çdo kamerë të fshehtë” vetëm duke skanuar Wi-Fi-n duhet të trajtohen me rezervë.

Po detektorët profesionalë?

Ekzistojnë pajisje që kërkojnë sinjale radiofrekuence ose reflektim optik të lentes.

Ato mund të ndihmojnë, por nuk janë të pagabueshme. Një detektor RF mund të reagojë ndaj telefonave, routerëve, Bluetooth-it dhe pajisjeve të tjera elektronike. Ndërsa një kamerë që regjistron vetëm në kartë memorie mund të mos transmetojë fare sinjal radio.

Prandaj mënyra më e mirë është kombinimi i kontrollit fizik, kontrollit optik dhe kontrollit të rrjetit, kur ky është i mundur.

Po apartamentet me qira?

Airbnb aktualisht nuk lejon kamera ose pajisje regjistrimi që monitorojnë hapësirat e brendshme të banesave të listuara në platformë, edhe nëse pajisjet janë të fikura ose të shkëputura. Kamerat e fshehta janë rreptësisht të ndaluara. Airbnb i përkufizon si pajisje regjistrimi edhe ato që regjistrojnë ose transmetojnë video, imazhe apo audio.

Kamerat e jashtme mund të lejohen sipas kushteve të platformës, por prania dhe vendndodhja e tyre duhet të deklarohen dhe ato nuk mund të monitorojnë zona ku njerëzit kanë pritshmëri të lartë për privatësi.

Nëse aieni në paalisie të dvshimtë

Mos e shkatërroni dhe mos e çmontoni menjëherë.

Fotografojeni pajisjen dhe pozicionin ku ndodhet. Dokumentoni ambientin dhe shmangni manipulimin e panevojshëm. Nëse mendoni se mund të bëhet fjalë për provë, mos hiqni kartën e memories dhe mos ndryshoni konfigurimet.

Në hotel ose apartament me qira, kontaktoni menaxhmentin ose platformën përmes së cilës është bërë rezervimi.

Nëse dyshoni se jeni regjistruar pa dijeninë tuaj në një hapësirë private, rasti mund t'u raportohet organeve kompetente dhe, kur kemi të bëjmë me përpunim të të dhënave personale, edhe Agjencisë për Informim dhe Privatësi.

Mos u përpiqni ta "hakoni" pajisjen për të zbuluar se kujt i përket dhe mos hyni në llogari ose sisteme që nuk janë tuajat.

Pesë gjëra që nuk duhet t'i merrni si të mirëqena

"Nëse nuk ka dritë të kuqe, nuk regjistron" – jo domosdoshmërisht.

"Nëse nuk ka Wi-Fi, nuk regjistron" – gabim; pajisja mund të ruajë pamjet lokalisht.

"Telefoni zbulon çdo kamerë" – jo.

"Një aplikacion mund ta gjejë çdo pajisje të fshehtë" – jo.

"Një kamerë e zakonshme shtëpiake është automatikisht e sigurt" – jo. Siguria varet edhe nga fjalëkalimi, firmware-i, llogaria, routeri dhe konfigurimi i qasjes nga larg. NCSC dhe FTC rekomandojnë masa konkrete për zvogëlimin e këtyre rreziqeve.

Nuk ekziston një "truk magjik" që zbulon çdo kamerë

Një pajisje mund të regjistrojë pa LED, pa zhurmë, pa Wi-Fi dhe pa dhënë shenja të dukshme.

Prandaj mbrojtja më e mirë është kombinimi i kontrollit fizik të ambientit, vëmendjes ndaj objekteve të pazakonta, kërkimit të reflektimeve, kontrollit për infra të kuqe dhe, kur është e mundur, kontrollit të rrjetit.

Privatësia sot nuk mbrohet vetëm duke kërkuar një lente të fshehur. Duhet menduar edhe për mikrofonin, lidhjen me internetin, ruajtjen e regjistrimeve, sigurinë e routerit dhe mbrojtjen e llogarive që kontrollojnë këto pajisje. /Telegrafi.

Të këshilluara



Nëna e braktisi, babai e dhunonte/ Sylvester Stallone bën rrëfimin e jetës

Nga New York Times/ Sylvester Stallone ka zënë një vend të madh në imagjinatën popullore për 50 vjet, që kur ai shpëtoi...



"Sytë e të dashuruarve"/ Çifti amerikan koleksionon bizhuteritë misterioze

Teksa po kërkonin sende antike, një sy i tërhoqi vëmendjen Davidit dhe Nan Skierit. Çifti amerikan po kërkonte "thesare&r...



Pamja këtu është e ri-koduar për ta futur në dokument. Artefakti autoritar është skedari WebP i ruajtur, dhe hash-i i tij është ai i shtypur te faqja e parë — pra dallimi është i verifikueshëm, jo i fshehur.