REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Analizë teknike
mbi
fushatën phishing përmes WhatsApp

Versioni: 1.0
Datë: 08/04/2025

Përmbajtja

Lista e figurave

Hyrje

Gjatë ditëve të fundit është evidentuar një fushatë aktive *Phishing* e cila qarkullon përmes platformës së komunikimit **WhatsApp,** duke u përhapur në mënyrë të shpejtë në Shqipëri. Kjo fushatë synon kompromentimin e llogarive të WhatsApp të përdoruesve përmes një skeme mashtruese që shfrytëzon besimin mes kontakteve të afërta dhe mungesën e njohurive për rreziqet e sigurisë kibernetike.

Mesazhi *phishing* dërgohet nga një kontakt i njohur në WhatsApp dhe përmban një tekst që fton përdoruesin të votojë për një vajzë në një "garë" fiktive për bursa shkollore, duke përfshirë edhe një **URL** mashtruese. Pasi viktima klikon në **URL**, ridrejtohet në një faqe që simulon një platformë votimi dhe i kërkon të vendosë numrin e telefonit si dhe autorizimin për llogarinë WhatsApp, duke përdorur një kod verifikimi me 8 karaktere.

Nëse autorizohet në WhatsApp-in e përdoruesit (*kodi i gjeneruar nga platforma phishing vendoset në whatsapp-in e përdoruesit*), aktorët keqdashës marrin akses të plotë në llogarinë WhatsApp të viktimës, të cilën e përdorin për të përhapur më tej fushatën dhe potencialisht për të mbledhur informacione sensitive të ruajtura në aplikacion.

Kjo fushatë phishing ka mashtruar një numër të konsiderueshëm qytetarësh, duke rezultuar në humbjen e kontrollit të llogarive të tyre WhatsApp.

Analiza Teknike

Gjatë analizës së kodit të faqes, evidentohet një pjesë kodi ***javascript***, nga ku kemi një funksion që bën ridrejtimin e përdoruesit në **URL**:

window.location.href = " *hxxps[://]danccenschoice[.]com/login/zomia-numberAL1*";

Pasi klikojmë në butonin **"autorizimi"**, do të evidentohet ndërfaqja tjetër si më poshtë ku kërkon të zgjidhet shteti dhe numri:

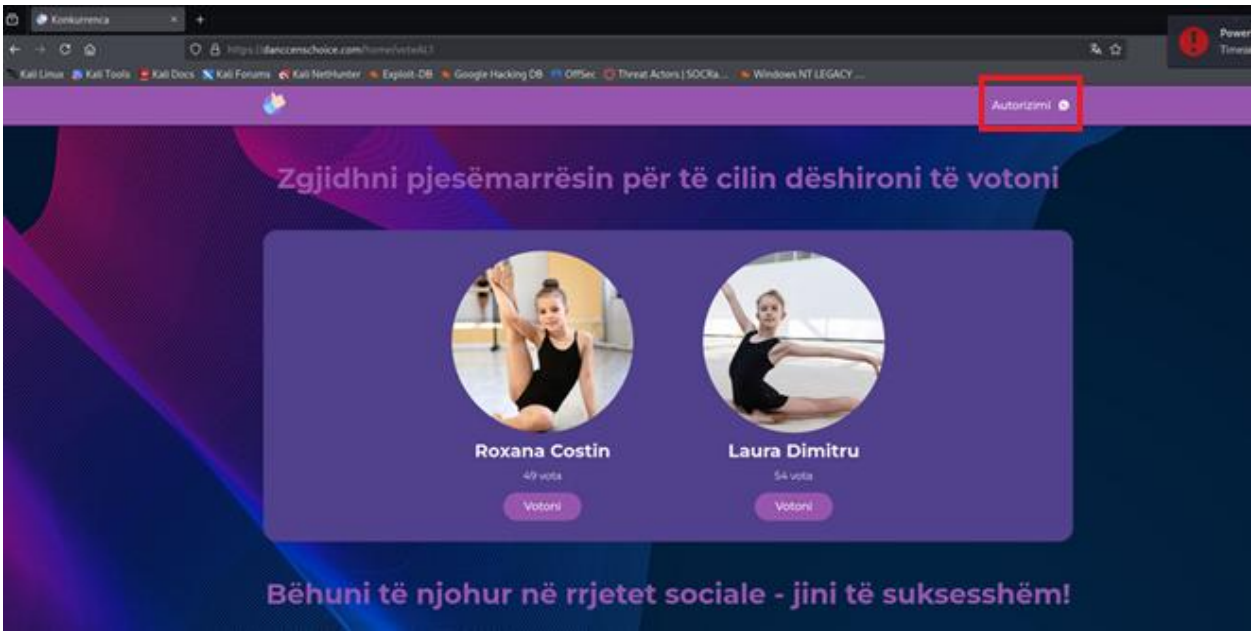

Figura 1. Aksesimi i ndërfaqes kryesore

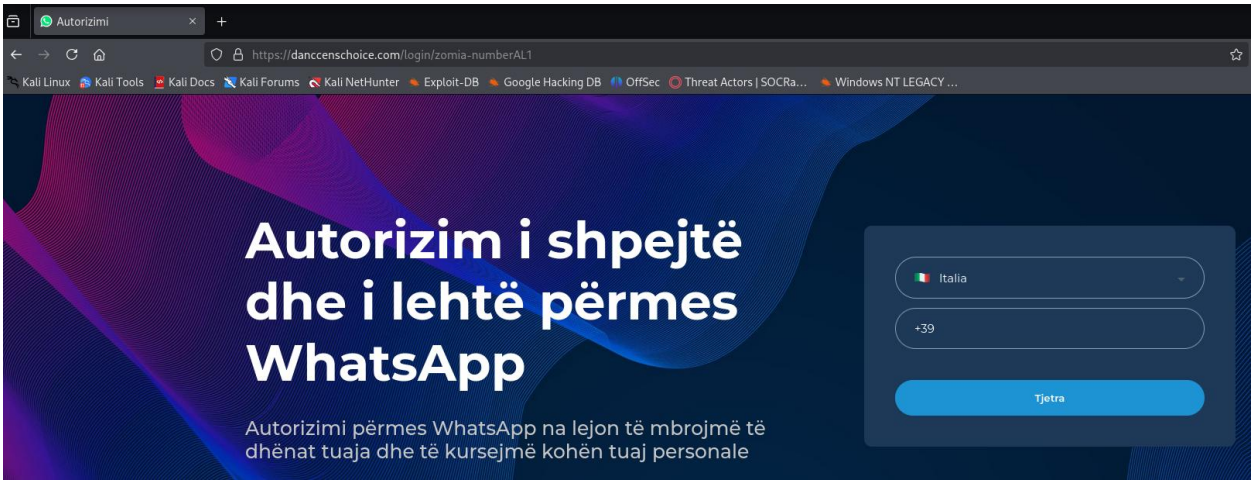

Figura 2. Ndërfaqja e autorizimit

Gjatë ngarkimit të faqes, nëse kontrollojmë trafikun ku kryhen thirrjet e aplikacionit do të evidentohen disa **URL**. Mund të përmendim URL **ipapi[.]co/json/**

Qëllimi i kësaj **URL** është të marrë informacione mbi vendndodhjen (**geolocation** dhe **IP**) e përdoruesit që po akseson këtë faqe.

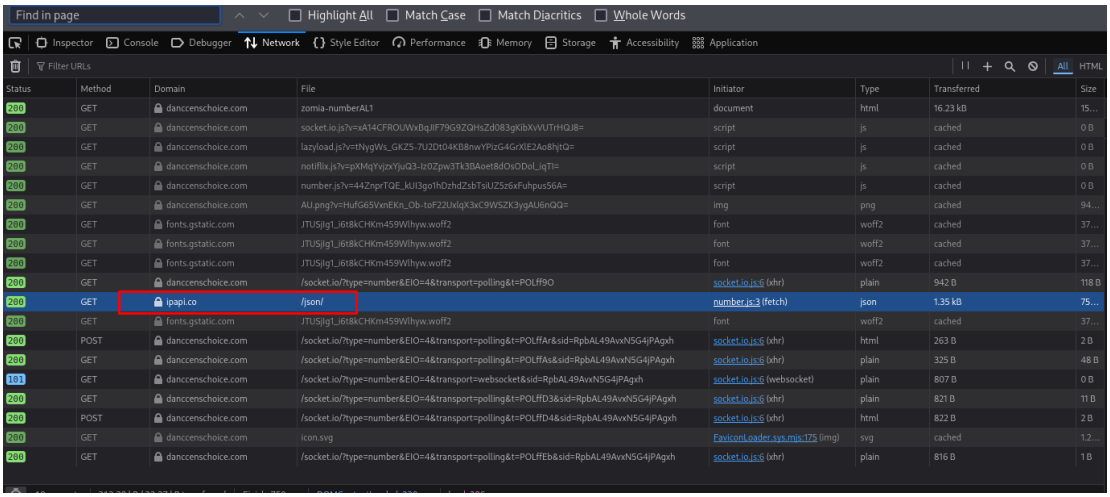

Figura 3. Kërkesa GET e URL ipapi.co

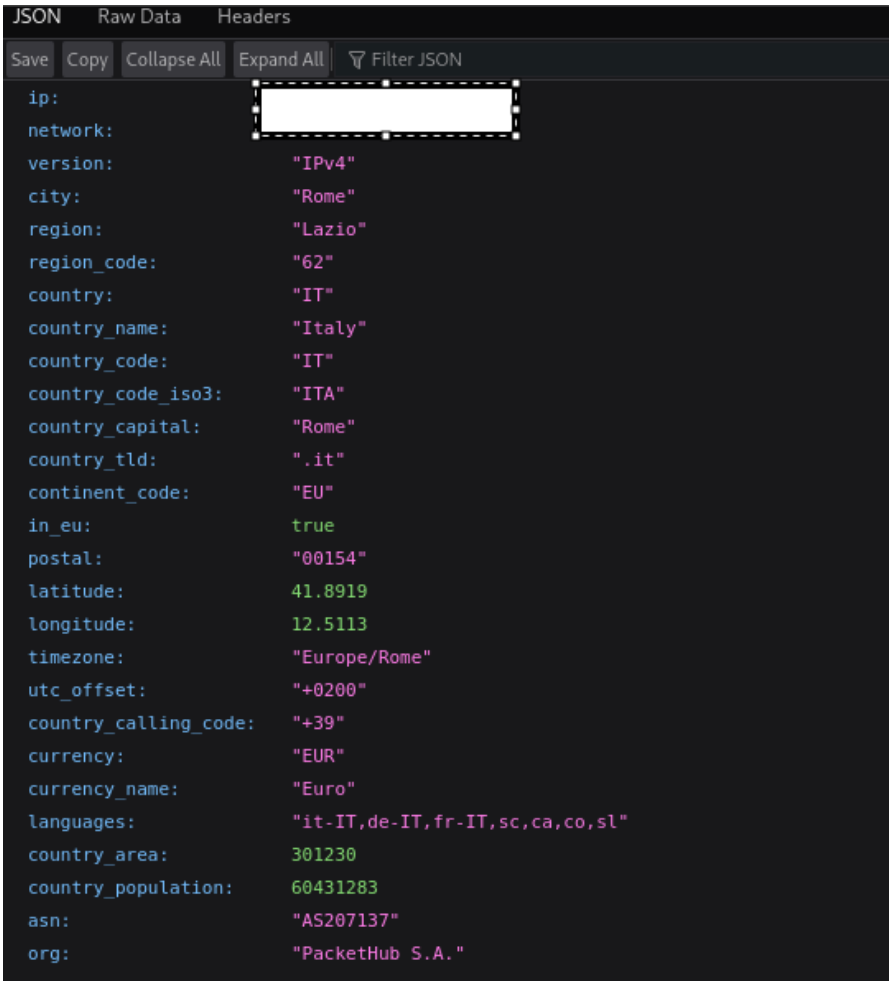

Figura 4. Pasi u aksesua domain-i ipapi.co

URL-të e tjera kanë në përmbajtje *socket.io.*

Socket është një librari në *javascript* e cila përdoret për **komunikim në kohë reale** midis klientit (zakonisht një faqe web) dhe serverit. Qëllimi i saj është që të bëhet vazhdimisht përditësimi i ndërfaqes së përdoruesit pa patur nevojë që faqja të rifreskohet.

Më tej, shohim kodin e ndërfaqes së autorizimit ku evidentohet një URL e cila përmban kodin javascript me emrin **number.js.**

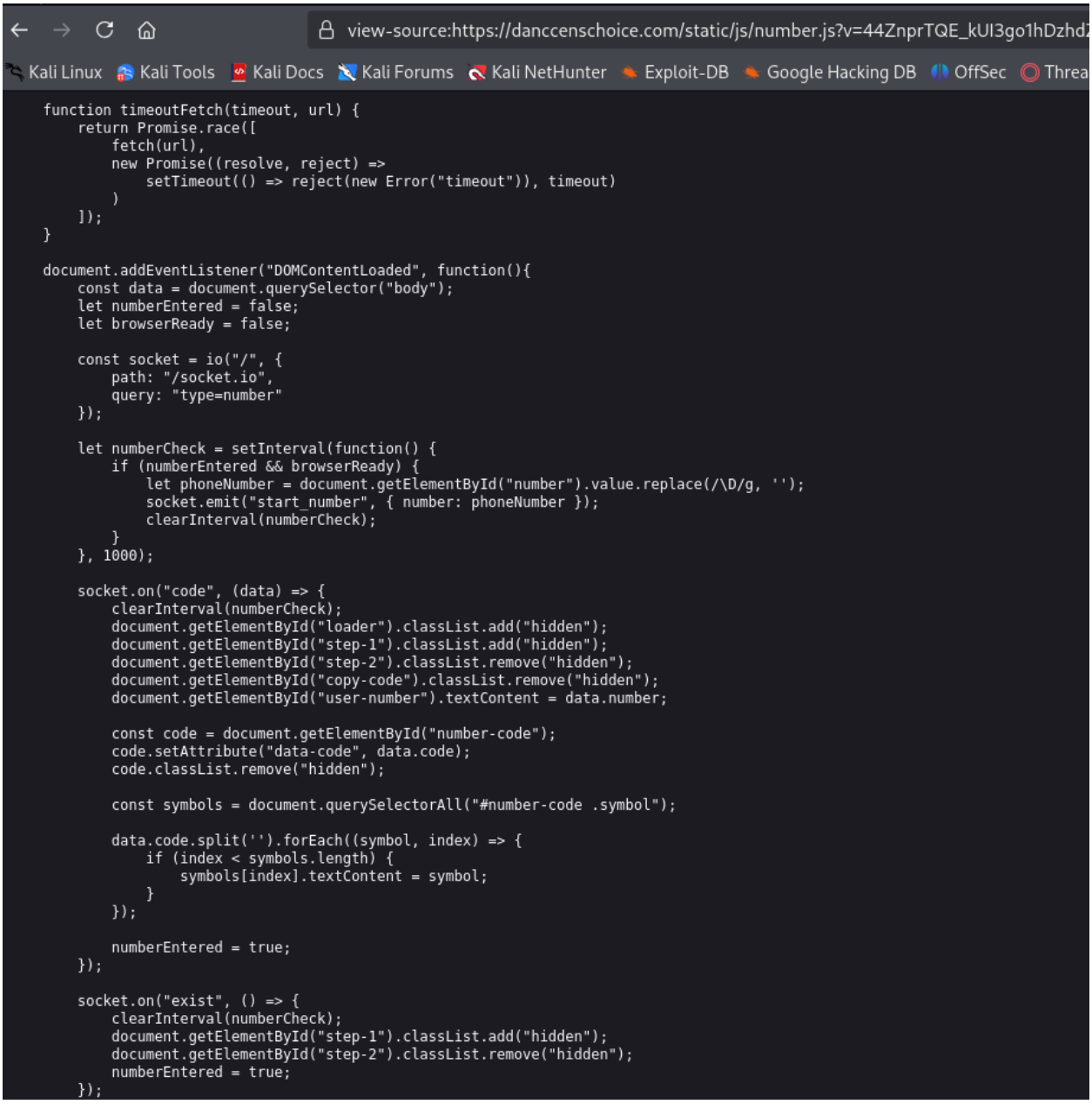

Figura 5. number.js

Në një shpjegim të përgjithshëm të kodit kemi ndërveprimin e **WebSocket** me serverin për të marrë në mënyrë të sinkronizuar përgjigjen që i vjen nga serveri ku është ngritur *webserver*-i i aktorëve keqdashës.

1. Në pjesën e kodit **let numberCheck** kemi një kontroll për të nisur dërgimin e numrit. Çdo sekondë kontrollohet nëse numri celular është plotësuar dhe nëse po, dërgon numrin përmes **socket** dhe e ndalon këtë interval.
2. **Socket.on(code,(data)=>{}** Kur **backend**-i dërgon një kod, ndërfaqja përditësohet për t'ia shfaqur atë përdoruesit.
3. **socket.on("exist", () => { ... });** Nëse numri egziston, e drejton përdoruesin në hapin e dytë (vendosja e kodit me 8 karaktere).

Gjithashtu dallohet dhe një event tjetër nga socket që ka emrin **surprise.**

socket.on("surprise", () => { ... });

Pasi vendosim një numër telefoni të simuluar klikojmë te butoni "***Tjetra***" në ndërfaqjen e autorizimit automatikisht do përditësohet faqja dhe do shfaqet një kod me 8 karaktere.

Gjithashtu përmbajtja e tekstit ndryshon dinamikisht duke u vendosur në tekstin :

"Shkoni te aplikacioni WhatsApp, zgjidhni "Pajisjet e lidhura" në dritaren e cilësimeve dhe më pas futni këtë kod. "

Kush është qëllimi i këtij kodi të gjeneruar si në kodin më poshtë ?

Figura 6. Faza pasi u vendos numri i telefoni dhe vendndodhja

Kodi që është gjeneruar shërben si urë lidhëse midis telefonit tuaj dhe kompjuterit të aktorëve keqdashës. WhatsApp ka një veçori që mund të shtohen pajisje që ta aksesoni atë përmes kompjuterit ose të një pajisjeje tjetër. Kjo realizohet nëpërmjet QR code ose me anë të **kodit** me 8 karaktere.

Në këtë rast nëse e shtojmë këtë kod në celularin tonë, automatikisht i japim qasje të plotë aktorëve keqdashës mbi WhatsApp-in tonë.

Funksionaliteti Legjitim

WhatsApp për përdoruesit e saj ofron që qasja në këtë platformë të bëhet edhe përmes Desktop-it apo Laptop-it. Si duket, është ky funksionalitet i cili shfrytëzohet nga sulmuesit për të fituar qasje të paautorizuar. Më poshtë forma legjitime.

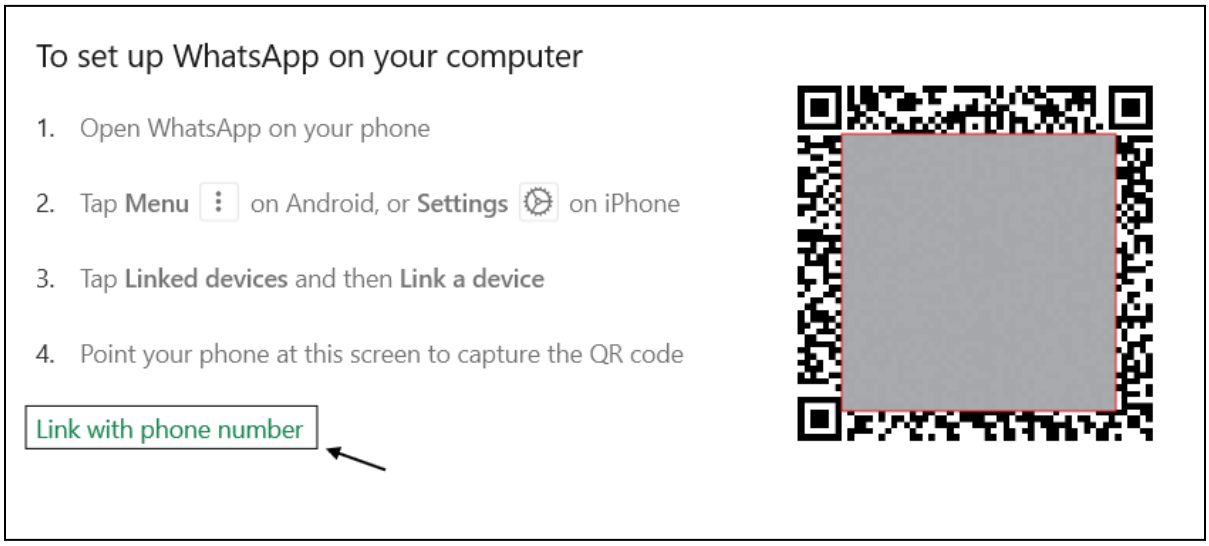

Figura 7. Lidhja e pajisjeve me numër telefoni

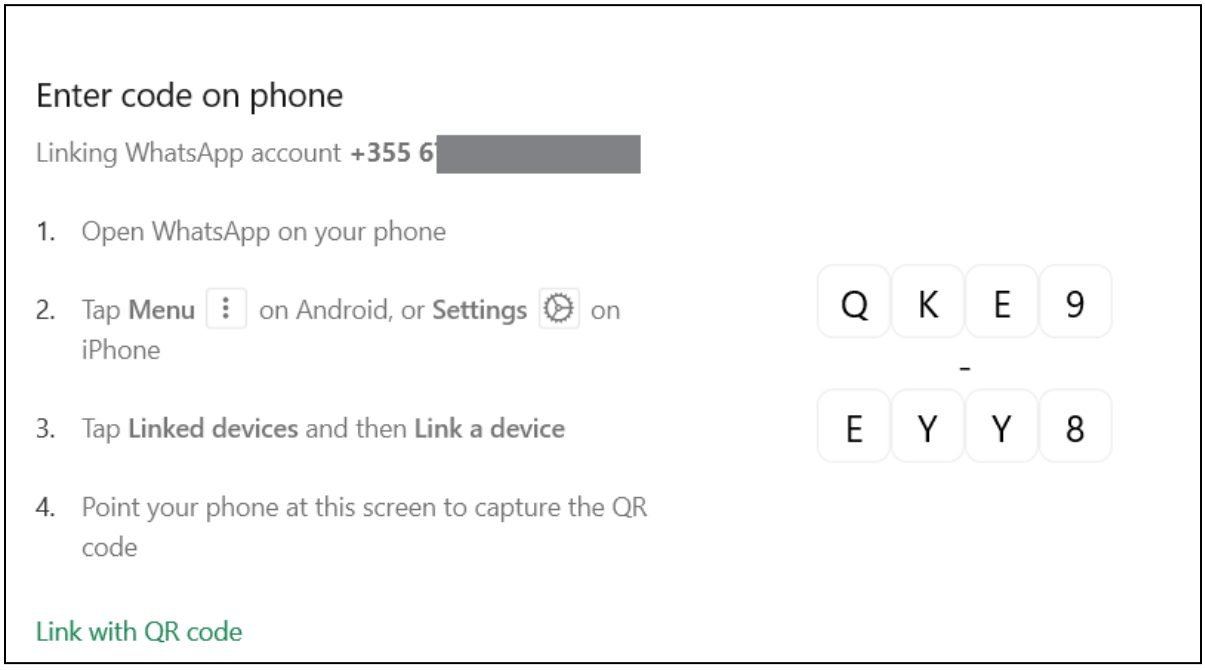

Figura 8. Kodi me 8 karaktere legjitim

Rekomandime

1. Për identifikimin e hyrjeve të paautorizuara, duhet që të shkoni tek ***Settings*** > ***Linked devices(referohu gjuhës aktuale të aparatit tuaj celular).*** Nëse keni pajisje të paautroizuara të lidhura me Whatsapp-in tuaj, çaktivizojini ato.

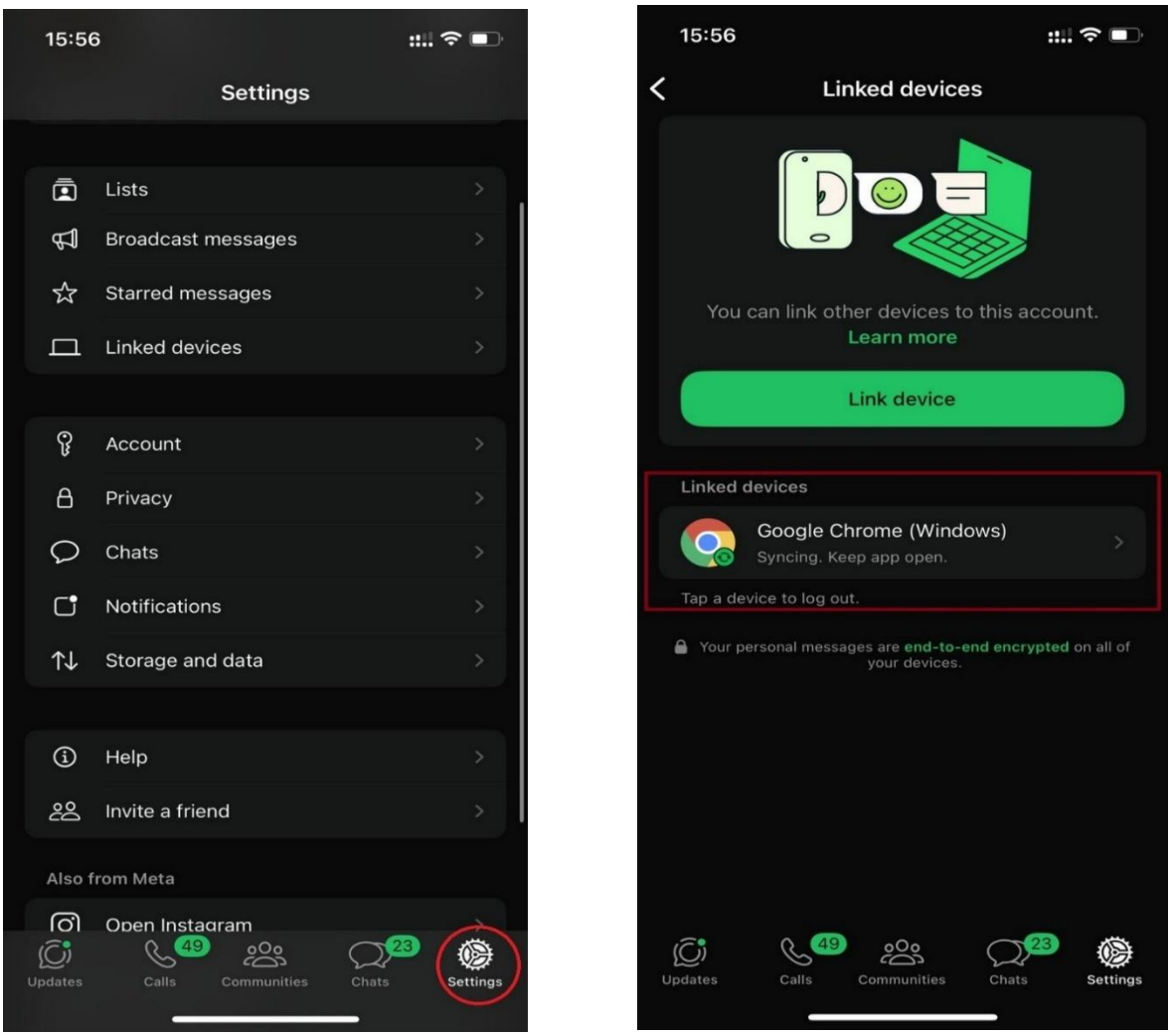

Figure 9 Çaktivizimi i pajisjeve të lidhura

2. Për qytetarët që janë bërë pjesë e kësaj skeme, rekomandohet që të rikthejnë menjëherë kontrollin mbi llogarinë e WhatsApp duke ndjekur procedurat zyrtare të rikuperimit dhe të ndërrojnë fjalëkalimet e llogarive të tjera të lidhura, si **Google Drive** apo **iCloud**. Gjithashtu, është e rëndësishme të njoftojnë kontaktet e tyre për kompromentimin dhe të shmangin shpërndarjen e mëtejshme të mesazhit.

3. Aktivizimi i MFA (Multi Factor Authentication – 2FA)