



EuskalHack Security Congress IX





No soy yo, pero te hackeo igual



#EuskalHack2026

No soy yo... pero te hackeo igual: explotación práctica con deepfakes

Porque nuestras caras ya no son tan seguras...

Sergio Mahía

Pentester @ KPMG



No soy yo, pero te hackeo igual



Me presento



Sergio Mahía

Pentester en KPMG

Divulgador de Ciberseguridad





No soy yo, pero te hackeo igual



¿Qué son los deepfakes?



No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual



- Poner tu cara en la cara de otro
- Saltarse sistemas de autenticación
- Normalmente se usan para cometer delitos

"Nadie que use mi cara está haciendo algo bueno" - Yo, 2026



No soy yo, pero te hackeo igual



¿Porque me importa esto a mi?





No soy yo, pero te hackeo igual



Europa Press · 1 año(s)

El volumen de vídeos deepfake online creció un 550% entre 2019 y 2023

Deloitte y Security Hero recogen ese crecimiento como señal de expansión acelerada del fenómeno ...

Yahoo Noticias en Español · 3 año(s)

Engañado y estafado por un falso Keanu Reeves creado con 'deepfake'

Agrega Yahoo como fuente de noticias preferida para ver más de nuestras historias en Google. La técnica del deepfake puede utilizarse con muchos fines: campañas publicitarias, 'revivir' a un ser ...

Autocasion · 1 año(s)

La IA casi le juega una mala pasada a Ferrari: su CEO fue víctima de un deepfake

Intento de estafa en Ferrari. A través de un deepfake, se ha intentado imitar la voz del CEO Benedetto Vigna en una llamada telefónica. La Inteligencia Artificial (IA) está desarrollándose a pasos ...



No soy yo, pero te hackeo igual



Montaje con el presunto agente de la RPDC durante la entrevista. Gemini - Omicrono

TECNOLOGÍA

Así cuela Corea del Norte a 'hackers' en empresas de todo el mundo: espían y financian al régimen de Kim Jong Un

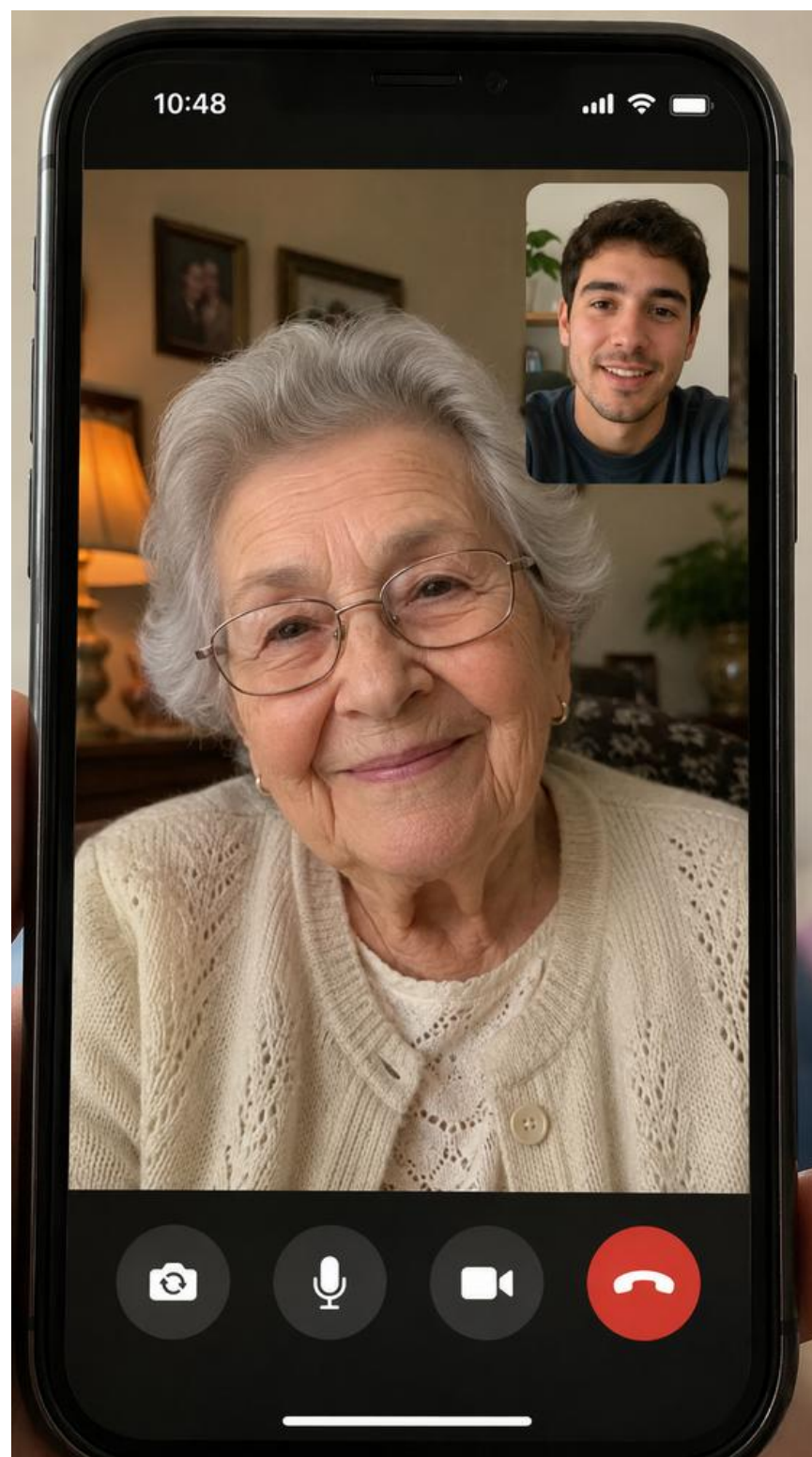
Recibe de lunes a viernes una clave sobre tecnología

Correo electrónico

☐ De conformidad con el RGPD, DE EL ESPAÑOL PUBLICACIÓN de datos facilitados con la finalidad de mantenerse actualizado.



No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual



Sergio, pero yo no tengo 87 años, a mi no me la
cuelan



No soy yo, pero te hackeo igual



Si tienes más de 1€ en el banco preocupate





No soy yo, pero te hackeo igual



¿Y cómo los hago yo?



No soy yo, pero te hackeo igual



Antes VS Ahora



- Ya no es necesario grandes unidades de cómputo
- No es “caro” en términos de generación
- Permite hacer deepfake “live”



No soy yo, pero te hackeo igual

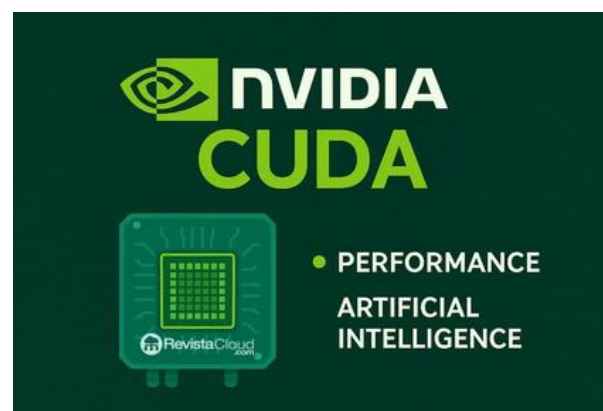




No soy yo, pero te hackeo igual



+



=

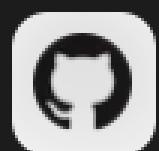




No soy yo, pero te hackeo igual



<https://github.com/hacksider/deep-live-cam>



GitHub

github.com > hacksider > deep-live-cam

GitHub - hacksider/Deep-Live-Cam: real time face swa...

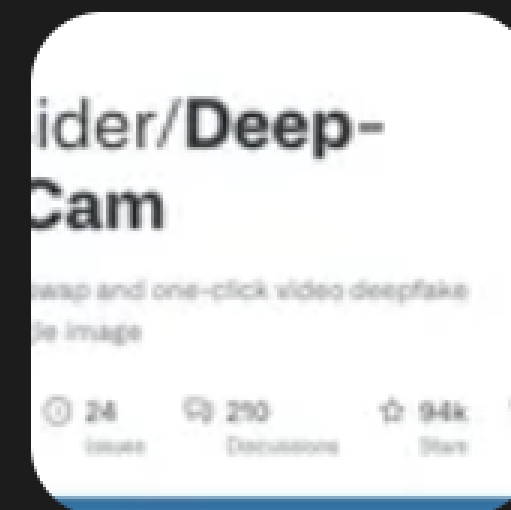
real time face swap and one-click video deepfake with only a single image

- hacksider/Deep-Live-Cam

Destacado por 93,9 mil Usuarios

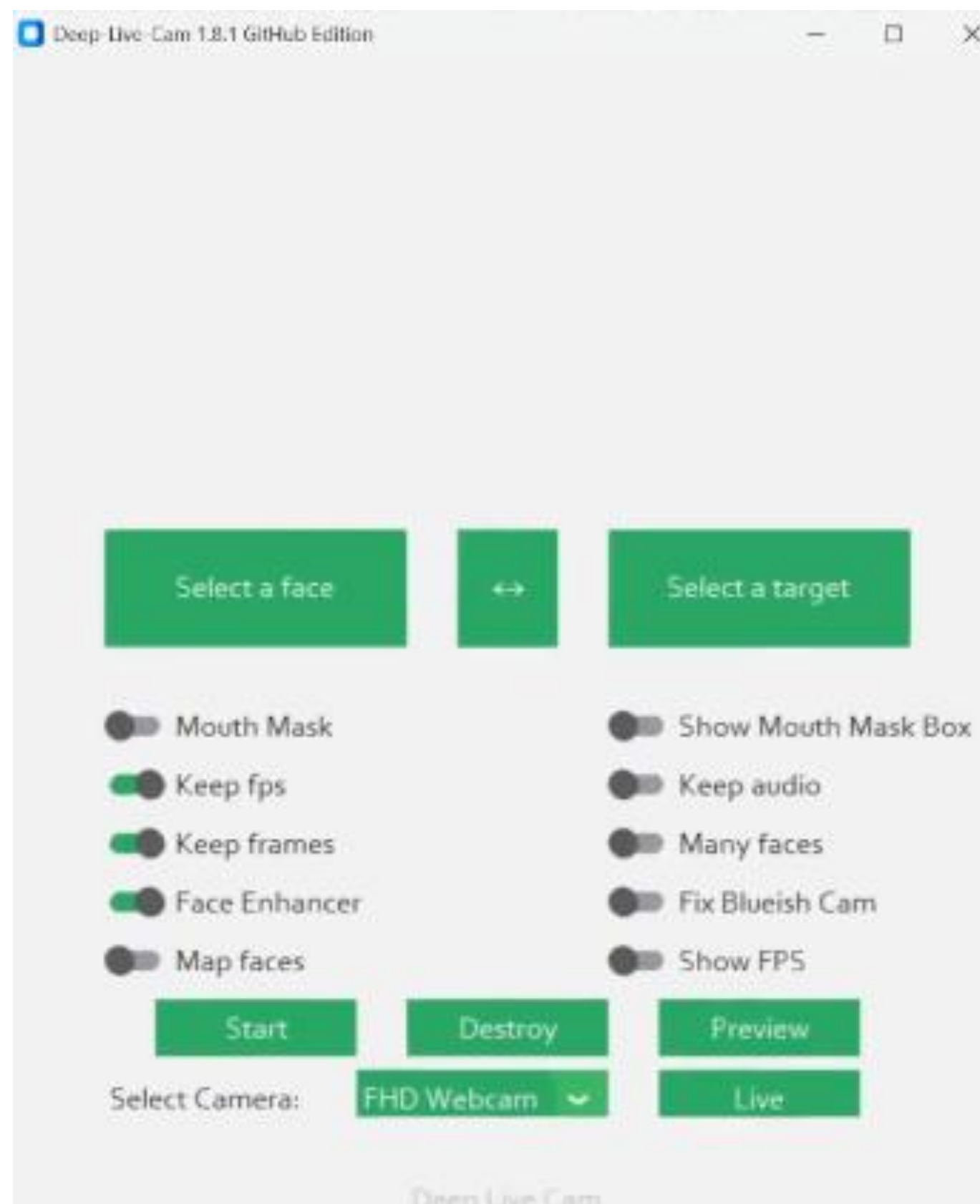
Forked por 13,7 mil Usuarios

Idiomas Python





No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual



¿Vemos ejemplos?



No soy yo, pero te hackeo igual



Todas las imágenes que se ven a continuación NO tienen el interés de ser ofensivas, solo, quizás de robar tu datos



No soy yo, pero te hackeo igual



¿Vemos ejemplos?





No soy yo, pero te hackeo igual



¿Cómo gestiona las emociones?



No soy yo, pero te hackeo igual



Enfado



Felicidad



Asombro



No soy yo, pero te hackeo igual



Incredulidad



Desprecio



Gran Asombo



No soy yo, pero te hackeo igual



¿Cómo gestiona la luz?



No soy yo, pero te hackeo igual



↑
Mi demonio de la
paralisis del
sueño



No soy yo, pero te hackeo igual



¿Cómo se lucha contra esto?



No soy yo, pero te hackeo igual



Detección en tiempo
real

```
    "width": 640
  },
  "capabilities": {
    "aspectRatio": {
      "max": 1920,
      "min": 0.000925925925925926
    },
    "deviceId": "241c1a7163b4758dfd8753ab1dd6b1",
    "facingMode": [],
    "frameRate": {
      "max": 60.000240325927734,
      "min": 0
    },
    "groupId": "1fac182f81e2e0116b081832993f036",
    "height": {
      "max": 1080,
      "min": 1
    }
  }
}
```

Análisis de metadatos



No soy yo, pero te hackeo igual



Análisis de metadatos

Cámara	Nombre sospechoso	Defecto	Máx.	FPS máx.	facingMode	Controles HW	1080p
OBS Virtual Camera	Sí	1080p60	1080p	60	Vacío	No	Sí
HP HD Camera	No	480p30	720p	30	user	Sí	No



No soy yo, pero te hackeo igual



Formas de evasión

```
    "width": 640
  },
  "capabilities": {
    "aspectRatio": {
      "max": 1920,
      "min": 0.000925925925925926
    },
    "deviceId": "241c1a7163b4758dfd8753ab1dd6b1",
    "facingMode": [],
    "frameRate": {
      "max": 60.000240325927734,
      "min": 0
    },
    "groupId": "1fac182f81e2e0116b081832993f036",
    "height": {
      "max": 1080,
      "min": 1
    }
  }
}
```

- Manipulación de metadatos del navegador
- Modificación de metadatos del sistema operativo
- Uso de drivers virtuales más avanzados
- Intermediación mediante hardware o capas externas



No soy yo, pero te hackeo igual



Formas de evasión

Nombre	Tipo	Datos
 (Predeterminado)	REG_SZ	(valor no establecido)
 CLSID	REG_SZ	{A3FCE0F5-3493-419F-958A-ABA1250EC20B}
 FilterData	REG_BINARY	02 00 00 00 00 00 20 00 01 00 00 00 00 00 00 00 30
 FriendlyName	REG_SZ	OBS Virtual Camera



No soy yo, pero te hackeo igual



Formas de evasión

VM227:3

(index)	kind	label	deviceId	groupId
0	'videoinput'	'OBS Virtual Camera'	'241c1a7163b4...'	'1fac182f81e2...'
1	'videoinput'	'HP HD Camera (0408:5349)'	'211f7ea60720...'	'191bebd34712...'

Array(2)

```
navigator.mediaDevices.enumerateDevices={()=>{const o=navigator.mediaDevices.enumerateDevices.bind(navigator.mediaDevices);return async()=>{return(await o()).map(d=>new Proxy(d,{get:(t,p)=>p=="label"&&/obs|virtual/i.test(t.label)?"HP HD Camera (0408:5349)":t[p]}))}}})();
```

VM234:3

(index)	kind	label	deviceId	groupId
0	'videoinput'	'HP HD Camera (0408:5349)'	'241c1a7163b4...'	'1fac182f81e2...'
1	'videoinput'	'HP HD Camera (0408:5349)'	'211f7ea60720...'	'191bebd34712...'

Array(2)



No soy yo, pero te hackeo igual



Formas de evasión



webrtcHacks

Technical information and experiments for WebRTC developers

Verified

142 followers Boston <http://webrtchacks.com> [@webrtchacks](#) admin@webrtchacks.com

Pinned

**adapter** Public

Shim to insulate apps from spec changes and prefix differences. Latest adapter.js release:

JavaScript 3.7k 860

**sdp-anatomy** Public

Source code for webrtcHacks' Anatomy of a SDP

JavaScript 91 24

**tfObjWebrtc** Public

Tensorflow Object Detection API Web Service wrapper that works on any <video> tag and WebRTC streams

Python 181 49

**aiy_vision_web_server** Public

Show camera feed and annotations of the AIY Vision Kit in a webpage

Python 46 13

**facetouchmonitor** Public

monitor how often you touch your face with WebRTC and tensorflow.js

**WebRTC-Camera-Resolution** Public

WebRTC Camera Resolution Finder



No soy yo, pero te hackeo igual



Formas de evasión

v4l2loopback - a kernel module to create V4L2 loopback devices

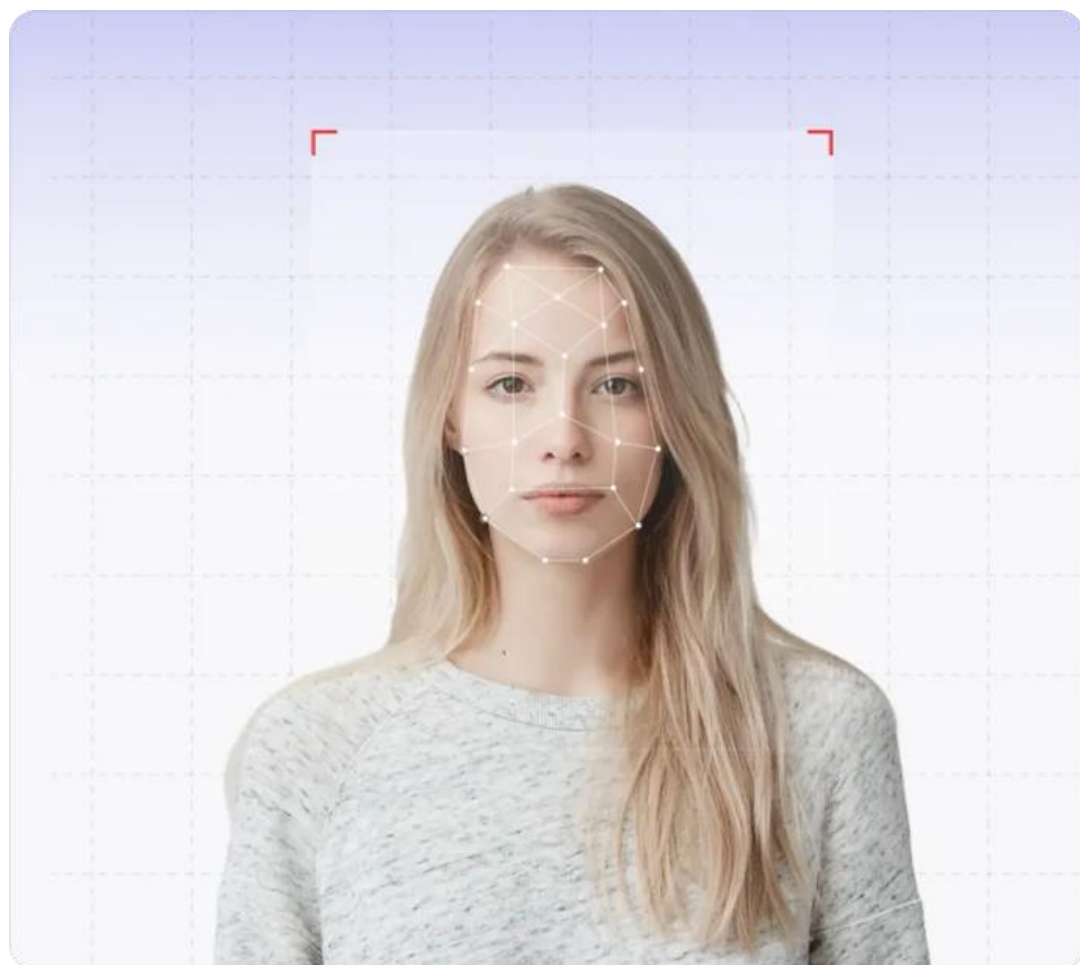
This module allows you to create "virtual video devices". Normal (v4l2) applications will read these devices as if they were ordinary video devices, but the video will not be read from e.g. a capture card but instead it is generated by another application. This allows you for instance to apply some nifty video effects on your Zoom video call... It also allows some more serious things (e.g. I've been using it to add streaming capabilities to an application by the means of hooking GStreamer into the loopback devices).



No soy yo, pero te hackeo igual



Formas de evasión



- Sistemas pensados para ser relativamente "laxos"
- Si son una operación bloqueante deben asumir riesgo en algunas ocasiones
- No siempre más es mejor, de hecho cuanto peor, mejor



No soy yo, pero te hackeo igual



Técnicas usadas para bypass



No soy yo, pero te hackeo igual



- Tasa de FPS -> Más bajo a veces da mejores resultados
- Calidad de la imagen -> Peor resolución mejores resultados
- Fondo -> A veces los fondos con movimiento aumentan ruido
- Género -> El resultado en ocasiones puede cambiar
- Etnias y edades -> algunas edad y etnias ofrecen mejores resultados





No soy yo, pero te hackeo igual



iiiLas empresas son vagas!!!

99% de las veces analizan metadatos





No soy yo, pero te hackeo igual



Casos de Uso



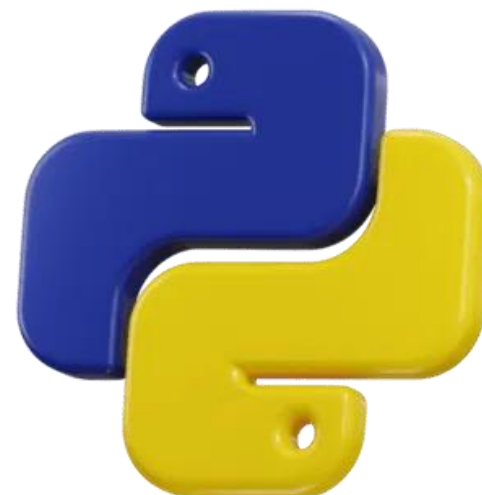
No soy yo, pero te hackeo igual



Bypass de verificación de edad
Ejercicio real en Banca



No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual

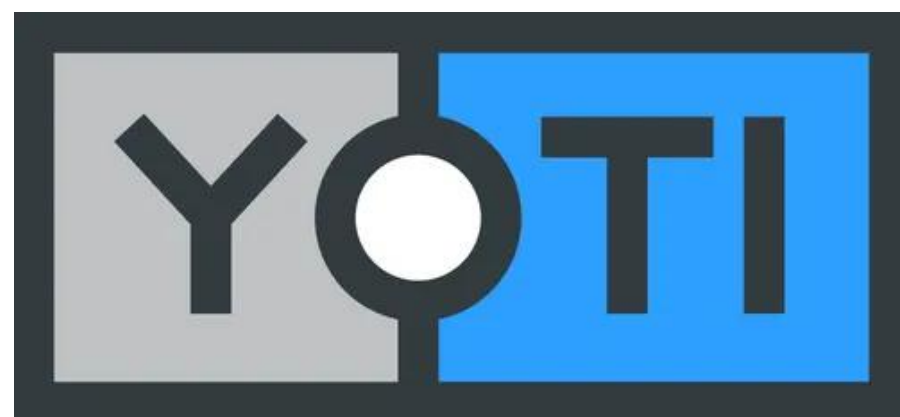


Bypass de verificación de edad





No soy yo, pero te hackeo igual



Over
10m
checks
every month



95%
Success
rate

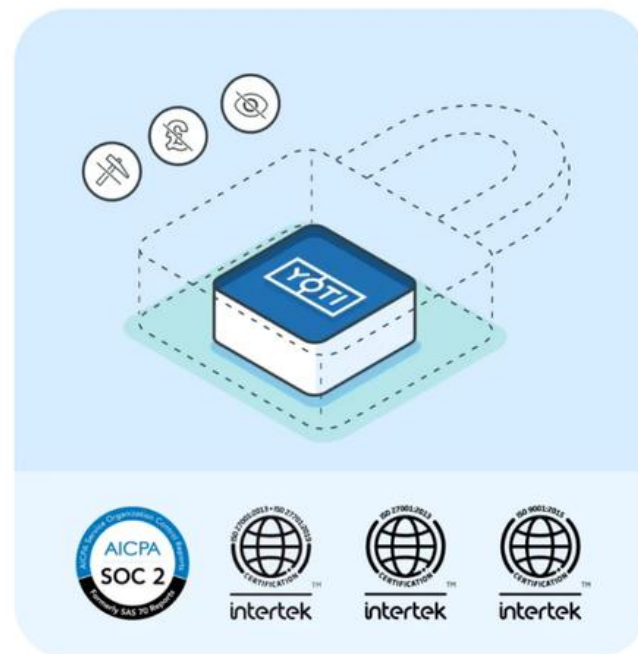


Building trust for market leaders

Yoti excels in building robust verification solutions for regulated businesses and governments



Scerling



Built with security and privacy as a priority

Our systems are built in a way that means we cannot mine or sell data to third parties. Once we've completed our security checks, we can't access any user details. We're trusted by regulators for adhering to the highest standards of security.



No soy yo, pero te hackeo igual



Its hackin' time





No soy yo, pero te hackeo igual



Bypass de verificación de edad

Basket 1 Item

The items in your basket are not reserved. Their availability may change.



John Lewis

Soft Grip Stainless Steel Serrated Utility Knife, 11.5cm

£8.00

You must be 18 or over to buy this item

We'll verify your age using facial age estimation at checkout.

[How to buy and return bladed items](#)

Quantity

-

1

+

Summary

Spend a further £62.00 to qualify for FREE Standard UK mainland delivery.

More delivery options at checkout

Total: £8.00
(excluding delivery)

Continue to checkout

Continue shopping

VISA

Mastercard

Apple Pay

Google Pay

AMEX

PayPal

clearpay

Klarna

Qatar

Age verification

We'll verify your age using facial age estimation

Please be ready to take a photo with the camera on your device.



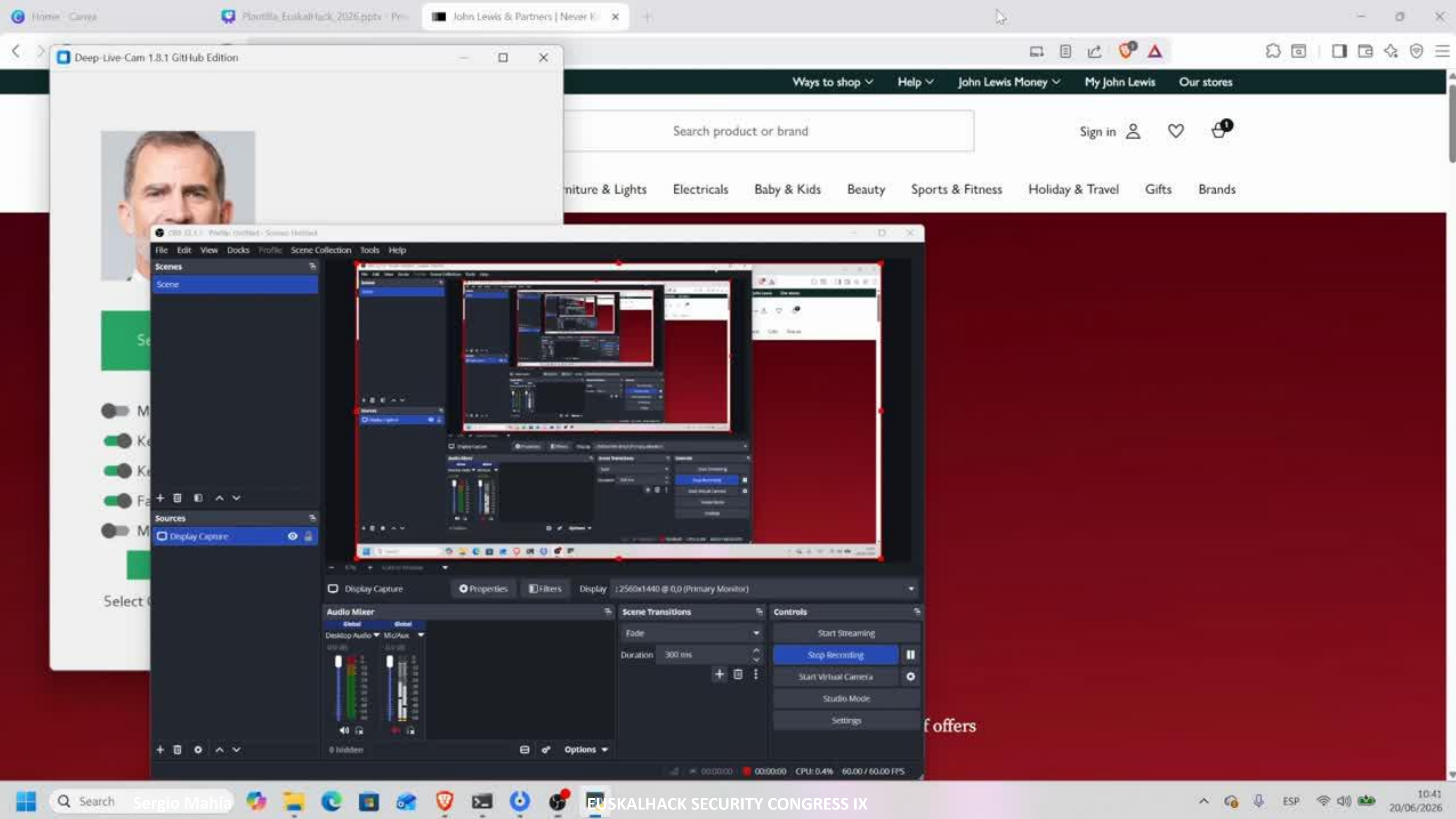
John Lewis Soft Grip Stainless Steel Serrated Utility Knife, 11.5cm

Quantity: 1

Return to basket

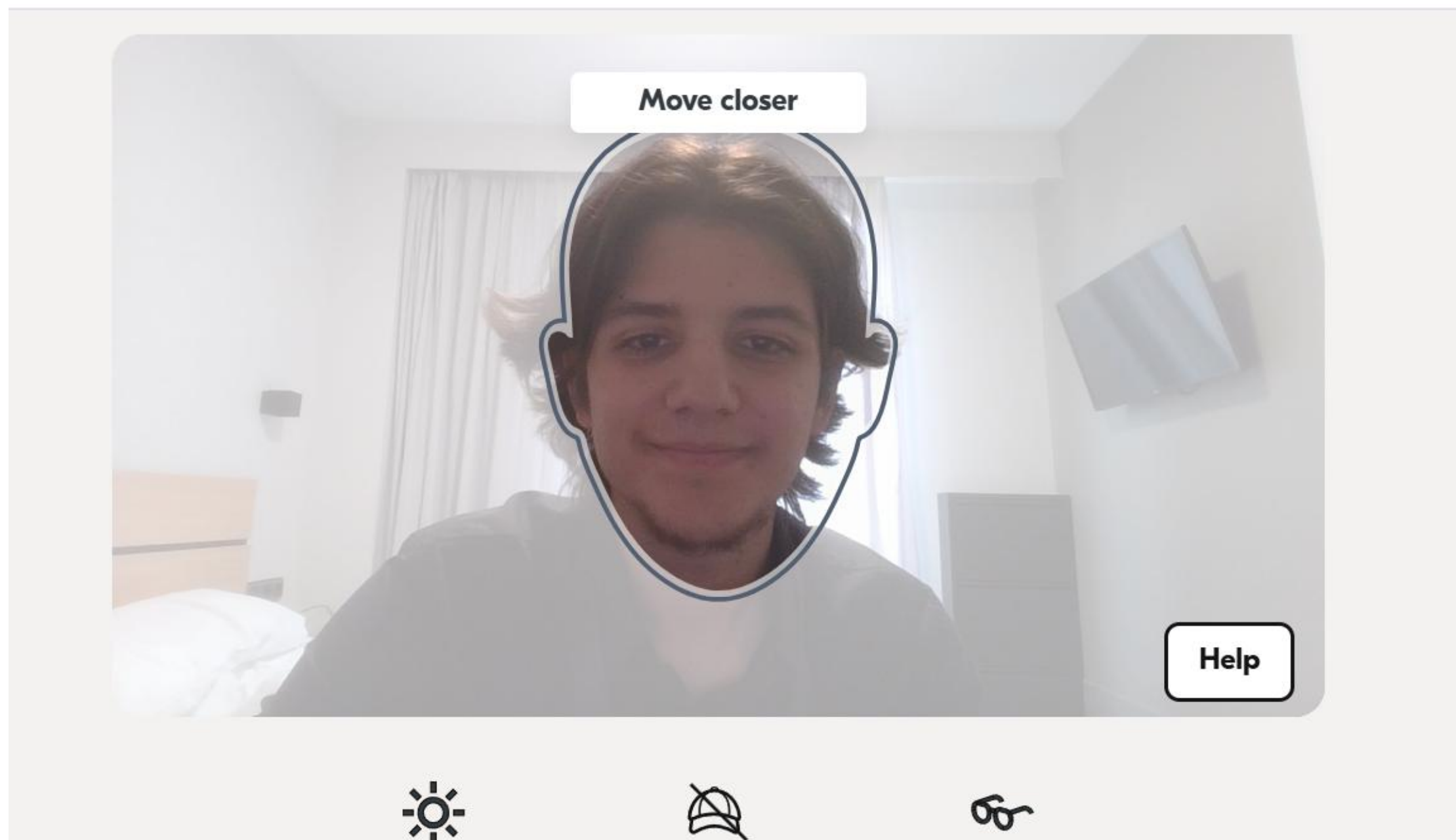
Verify your age

powered by YOTI





No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual



**We could not
confirm you meet
the required age**

Try confirming your age with Age
estimation again, or use another
method.

i You have 1 more attempt to
confirm your age with Age
estimation.

Try again

Select another method

Cancel age check



No soy yo, pero te hackeo igual



Registro bancario



No soy yo, pero te hackeo igual

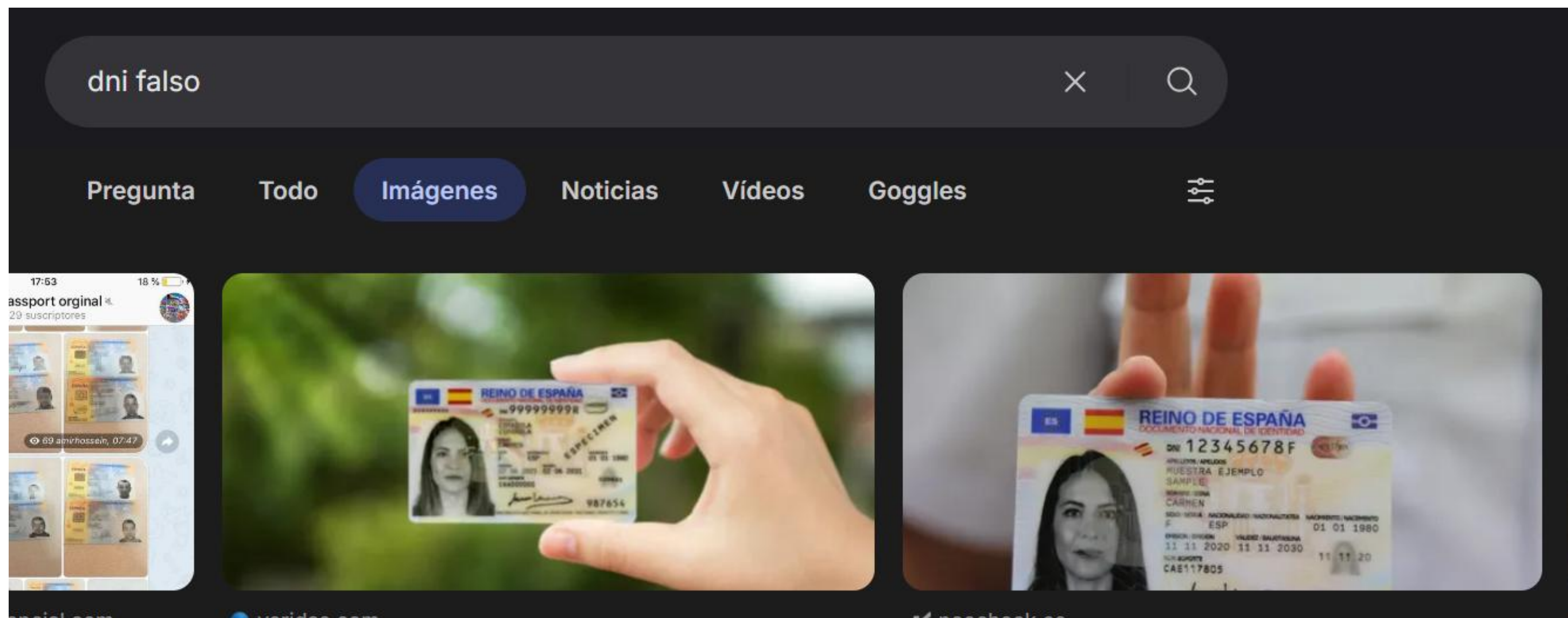


Requisitos

- DNI
- Deepfake con DNI por ambas caras
- Liveness detection



No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual



Solo tengo esta foto de mi madre antes de morir, mejora la calidad y hazla realista. Es de su carnet de conducir





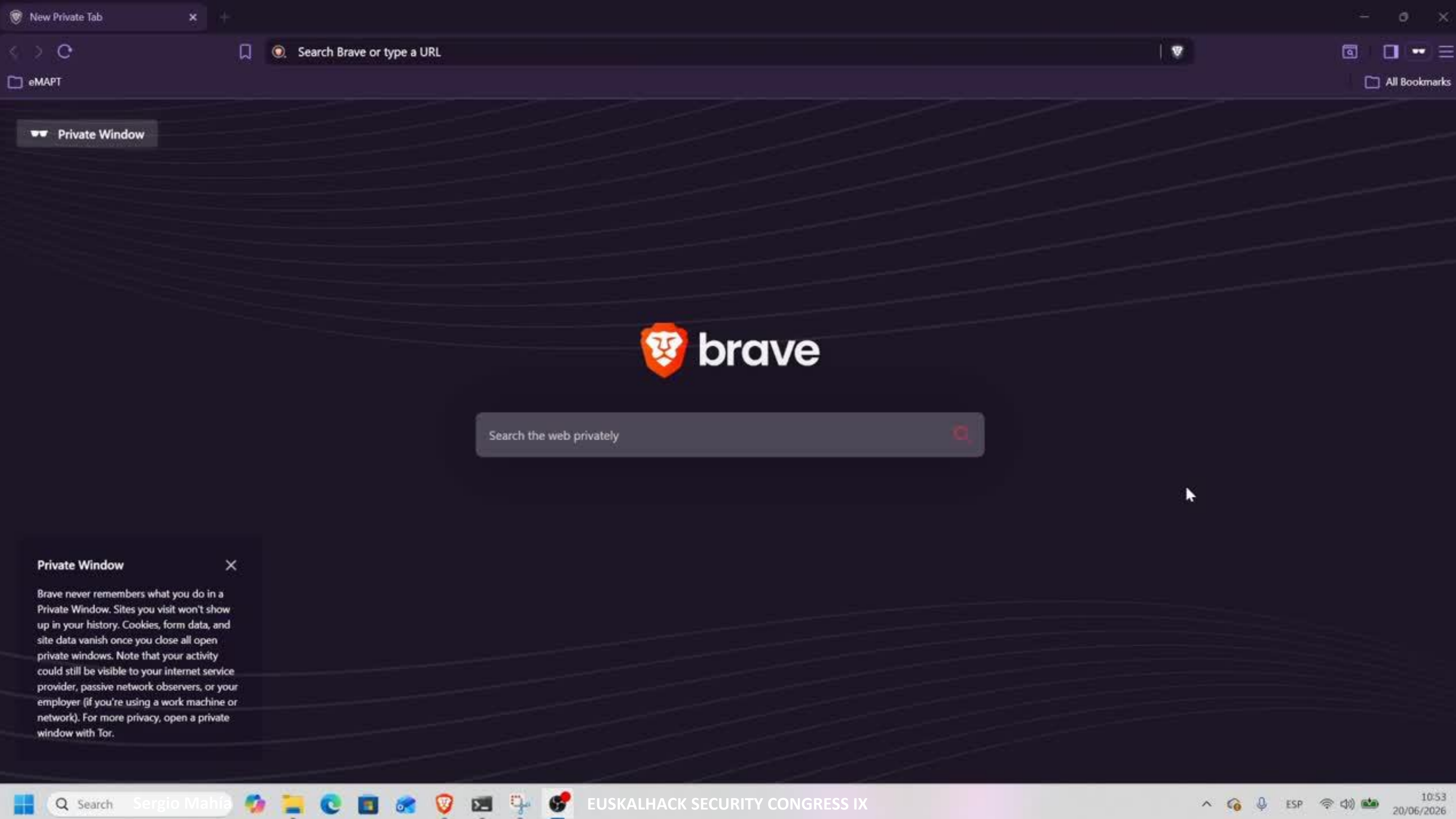


No soy yo, pero te hackeo igual

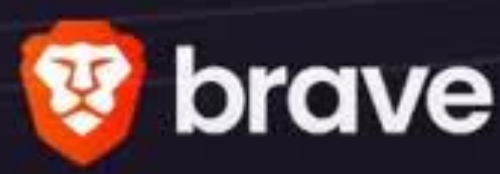


Nuestra víctima





Private Window



Search the web privately

Private Window

Brave never remembers what you do in a Private Window. Sites you visit won't show up in your history. Cookies, form data, and site data vanish once you close all open private windows. Note that your activity could still be visible to your internet service provider, passive network observers, or your employer (if you're using a work machine or network). For more privacy, open a private window with Tor.



No soy yo, pero te hackeo igual



Ingeniería social



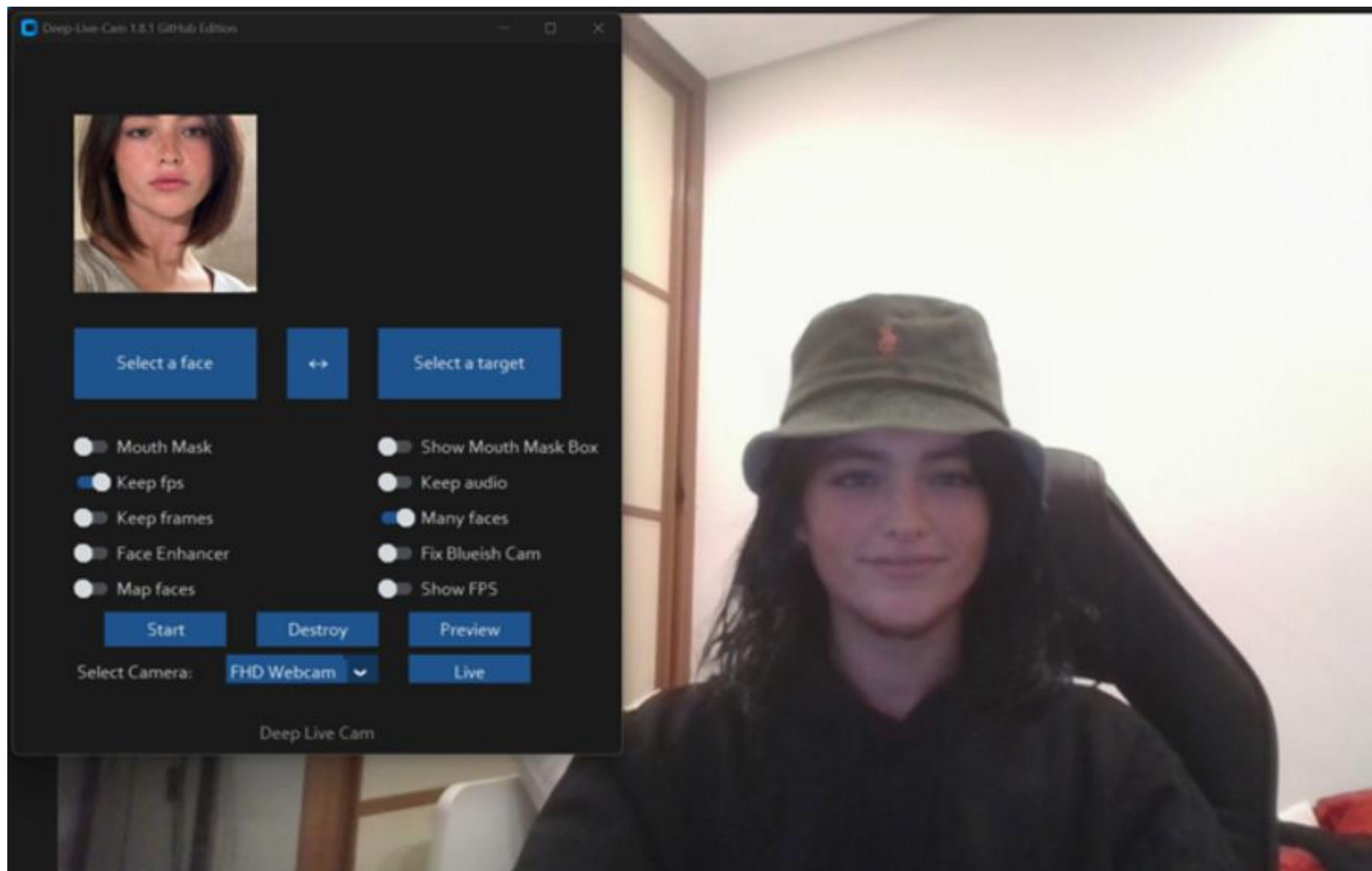
No soy yo, pero te hackeo igual



Os presento a Serg-IA



No soy yo, pero te hackeo igual

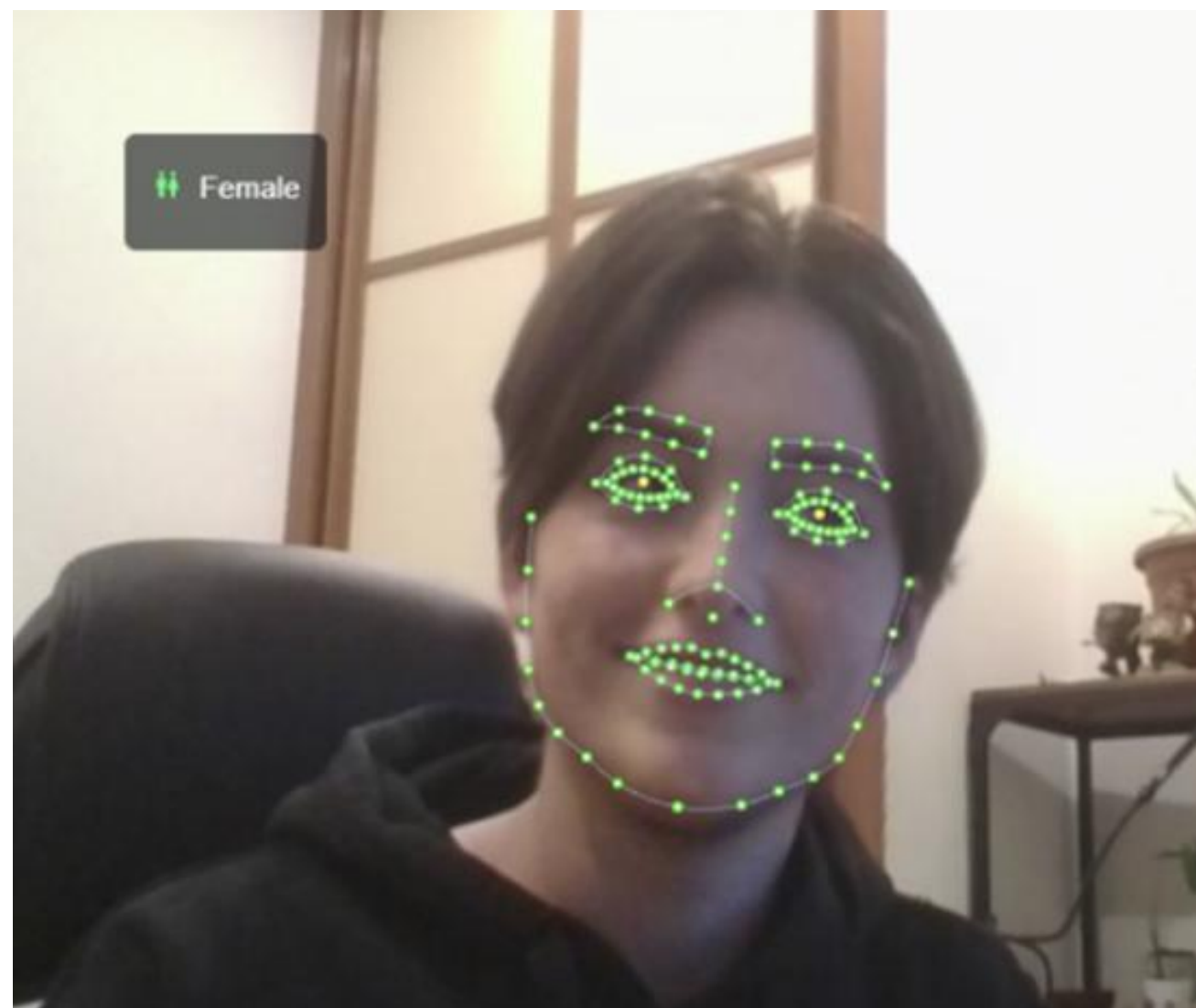




No soy yo, pero te hackeo igual



Detección de género



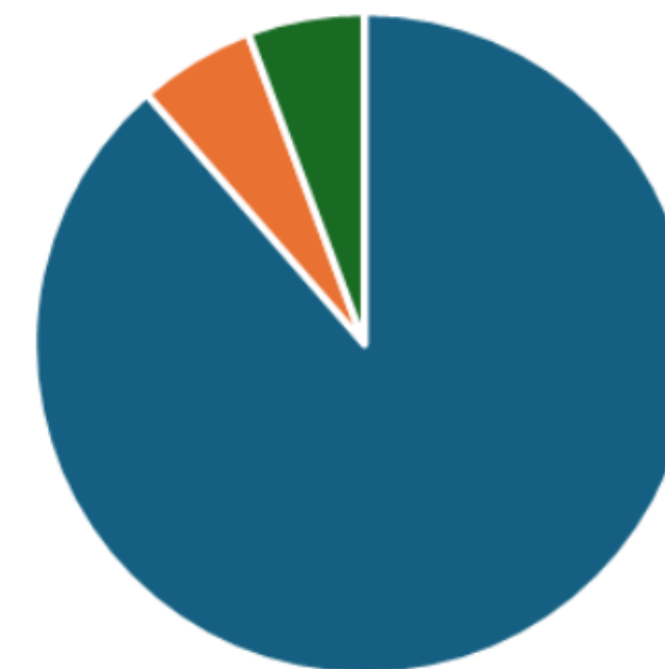


No soy yo, pero te hackeo igual



chatroulette
Meaningful Connections

Resultados Credibilidad Deepfake

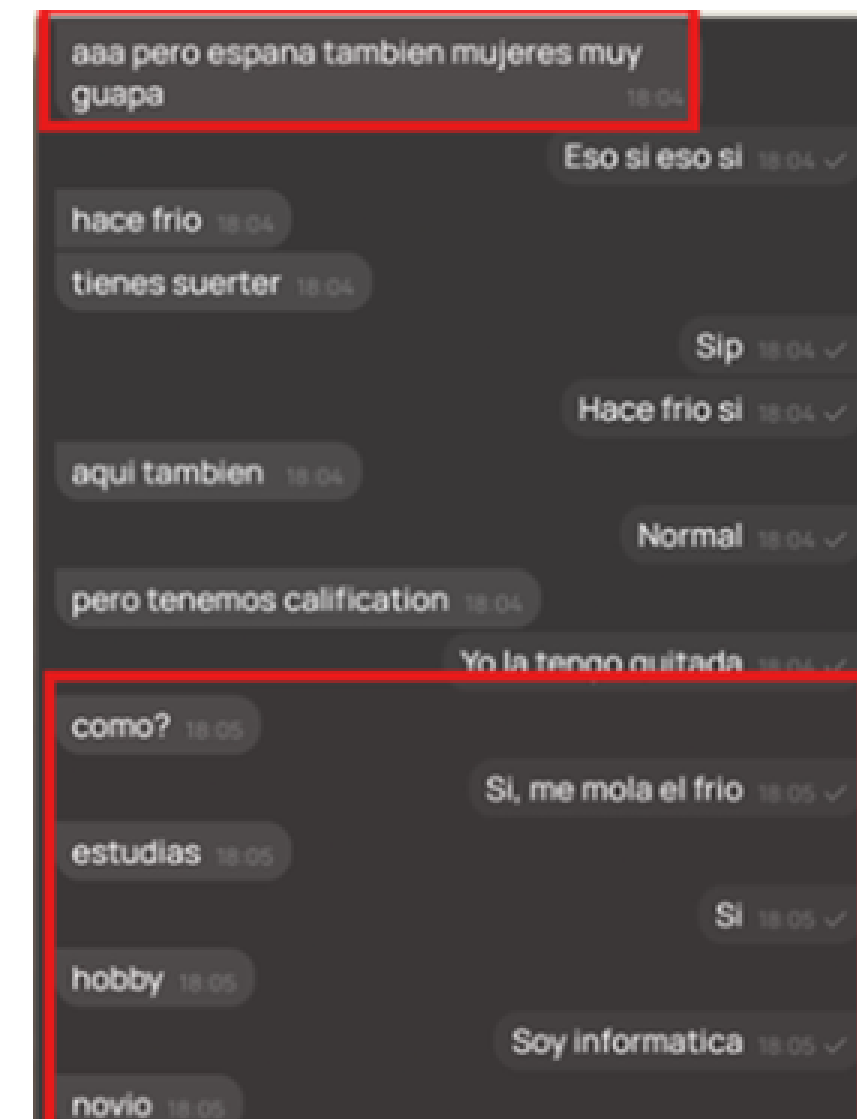
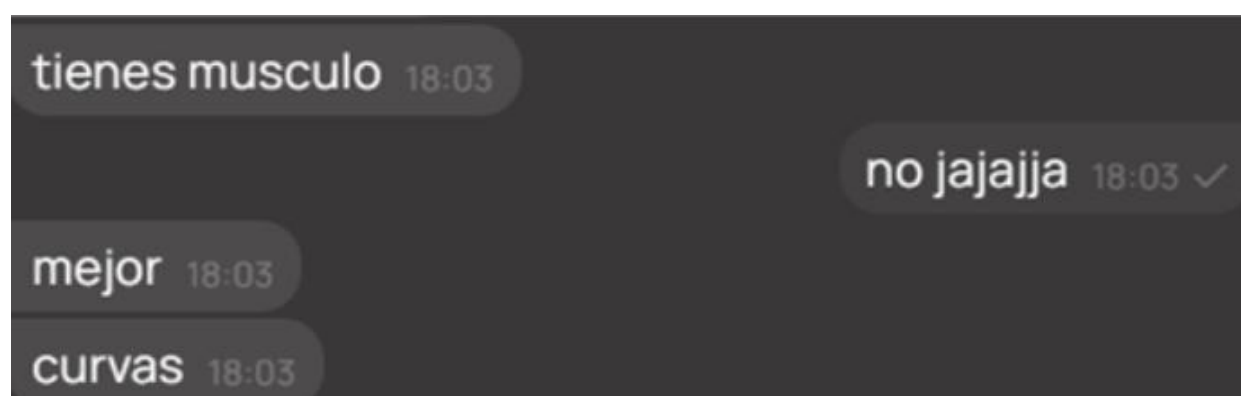
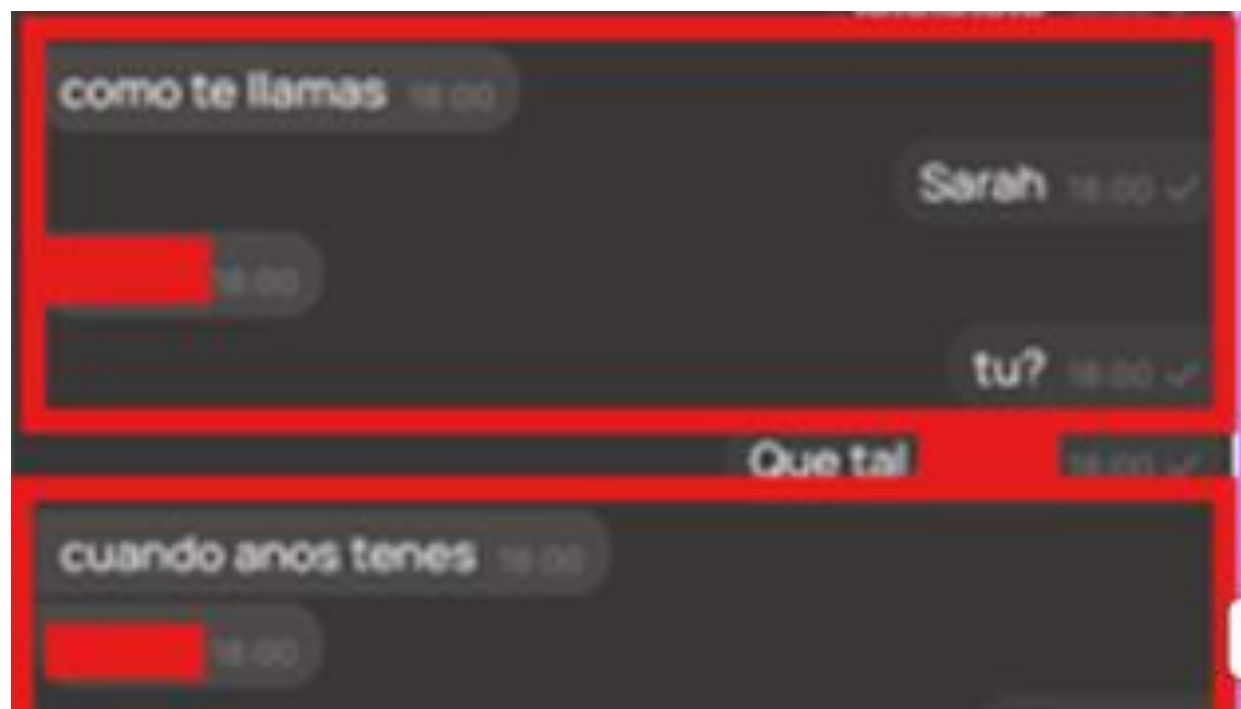


■ SI ■ MAS O MENOS ■ NO

28-SI 2-PUEDE 2-NO



No soy yo, pero te hackeo igual





No soy yo, pero te hackeo igual



En resumen... tiene mala pinta





No soy yo, pero te hackeo igual



!!Muchas gracias!!
ESKERRIK ASKO!

sergio.mahiarello@gmail.com

<https://www.linkedin.com/in/sergio-mahia/>



Sergio Mahía

Software Developer | Cybersecurity
| Ethical Hacking | Red Team | Pentest...





Título de la charla



¡MUCHAS GRACIAS!
ESKERRIK ASKO!

