



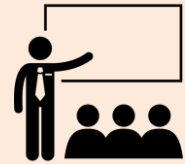
C-DAYS

2025

Agenda



Disclaimer & Legal Considerations



Presentation is solely for educational and awareness purposes.



Live content may be unpredictable and potentially inappropriate for some viewers.



Users must check the legality of OSINT tools and methods in their country.

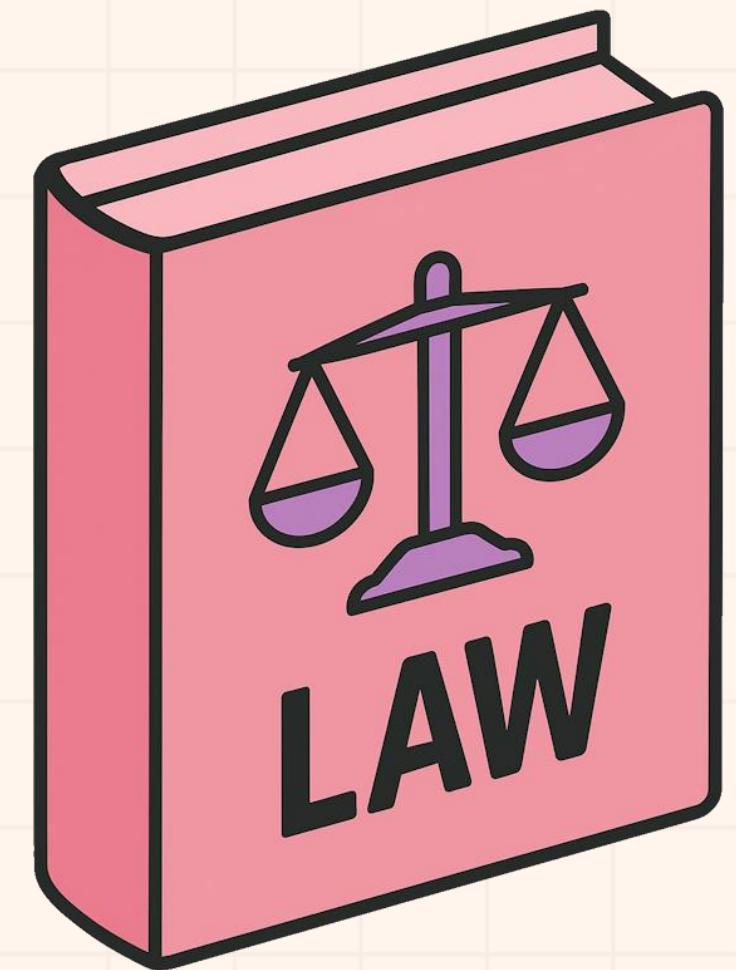


This presentation is not related to my work or employer.



Disclaimer & Legal Considerations

- **Portuguese Law**
 - Diário República Eletrónico ([link](#))
 - ANACOM ([link](#))
- **Organizations**
 - CNCS – Centro Nacional de Cibersegurança ([link](#))
 - Incident Notification ([link](#))
 - CERT.PT ([link](#))
 - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#))
 - Ministério Público ([link](#))



Disclaimer & Legal Considerations

ARTIFICIAL INTELLIGENCE

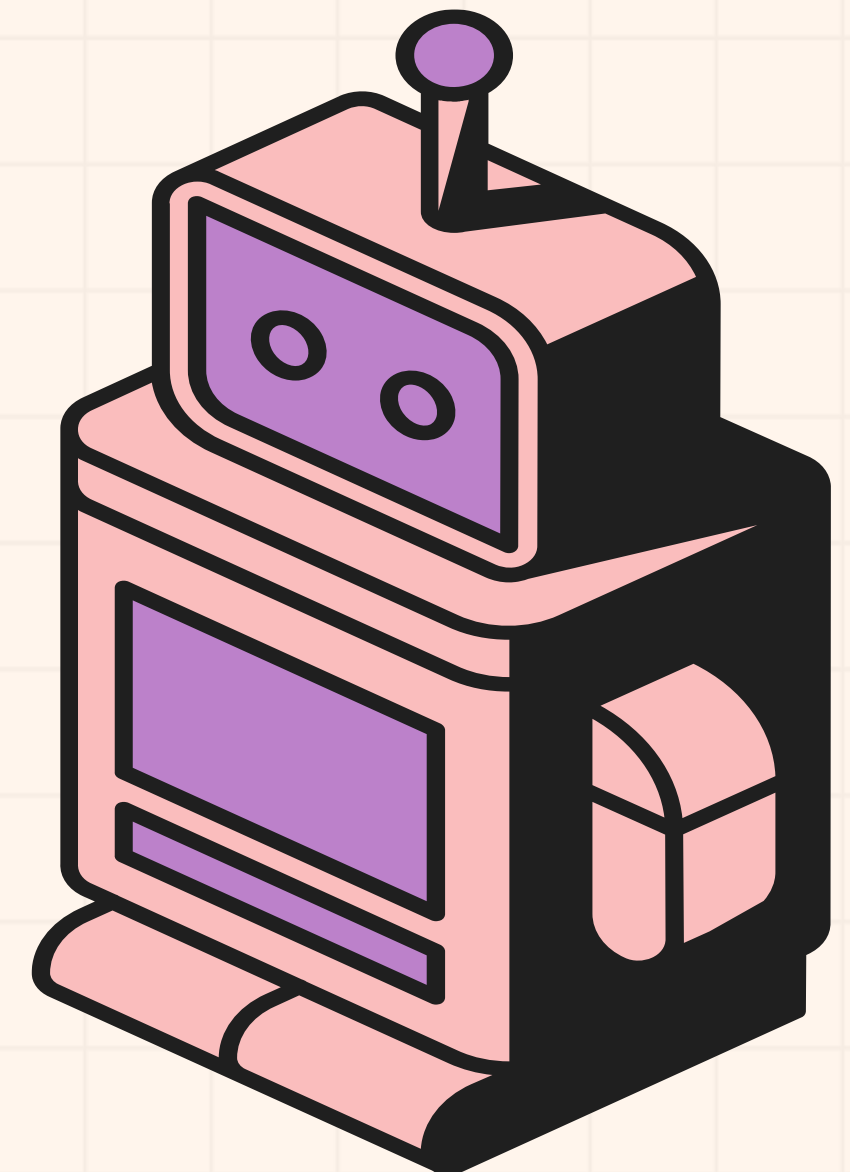
Was heavily used for this presentation

Use available technologies but check facts.

Always check facts.

AI is more than ChatGPT. Grok, Claude, ...

Use them all.



\$whoami

🕶️ Pedro António Oliveira Vieira

🔒 Cybersecurity Engineer

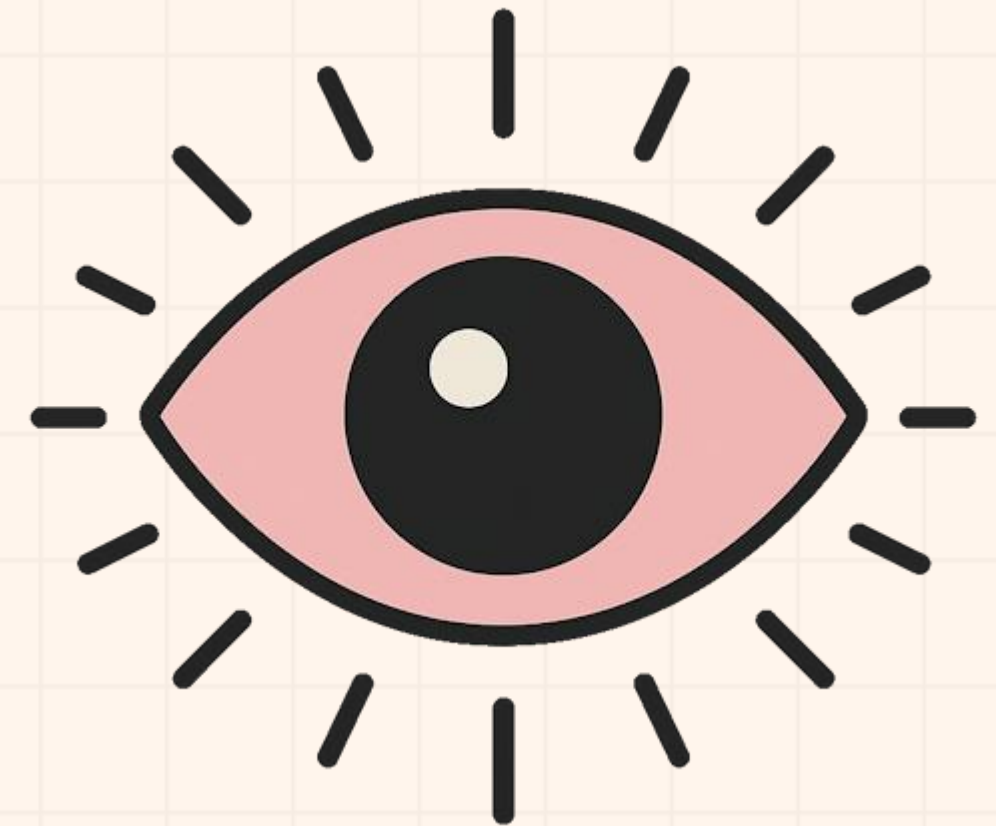
🕵️ OSINT

🖋️ Full stack developer

👤 Public Speaker



AWARENESS



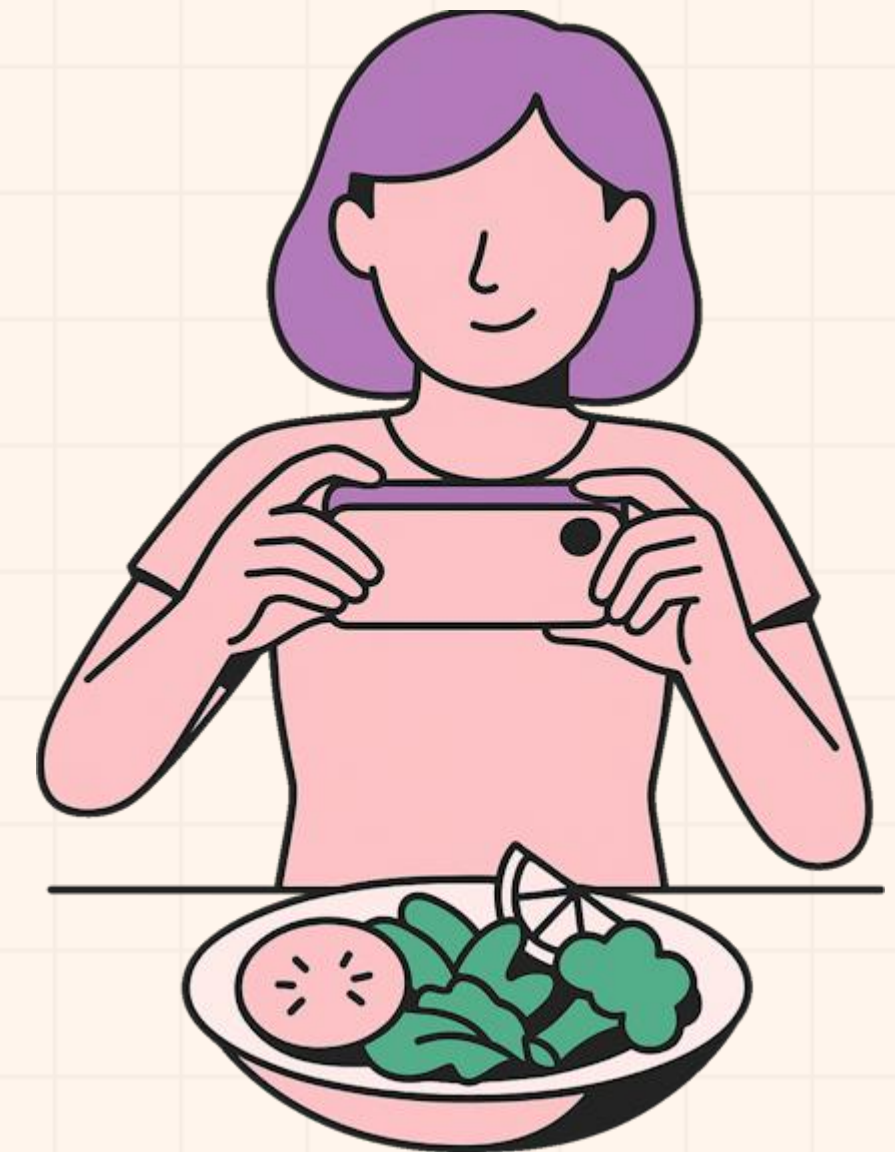
Awareness - True stories – Quiet vacations

- Long last deserving vacations
 - Too many friends at destination
 - So, warn no one and just relax on vacations
- I posted a picture on social media
 - My friends were alerted I was nearby
 - Friends on that location called me on the phone
 - Everyone else knew I was not home
 - **Burglars love that kind of information**
 - Not public profile. At least I think it is not (rules change)
 - Someone could have shared the photo with the world



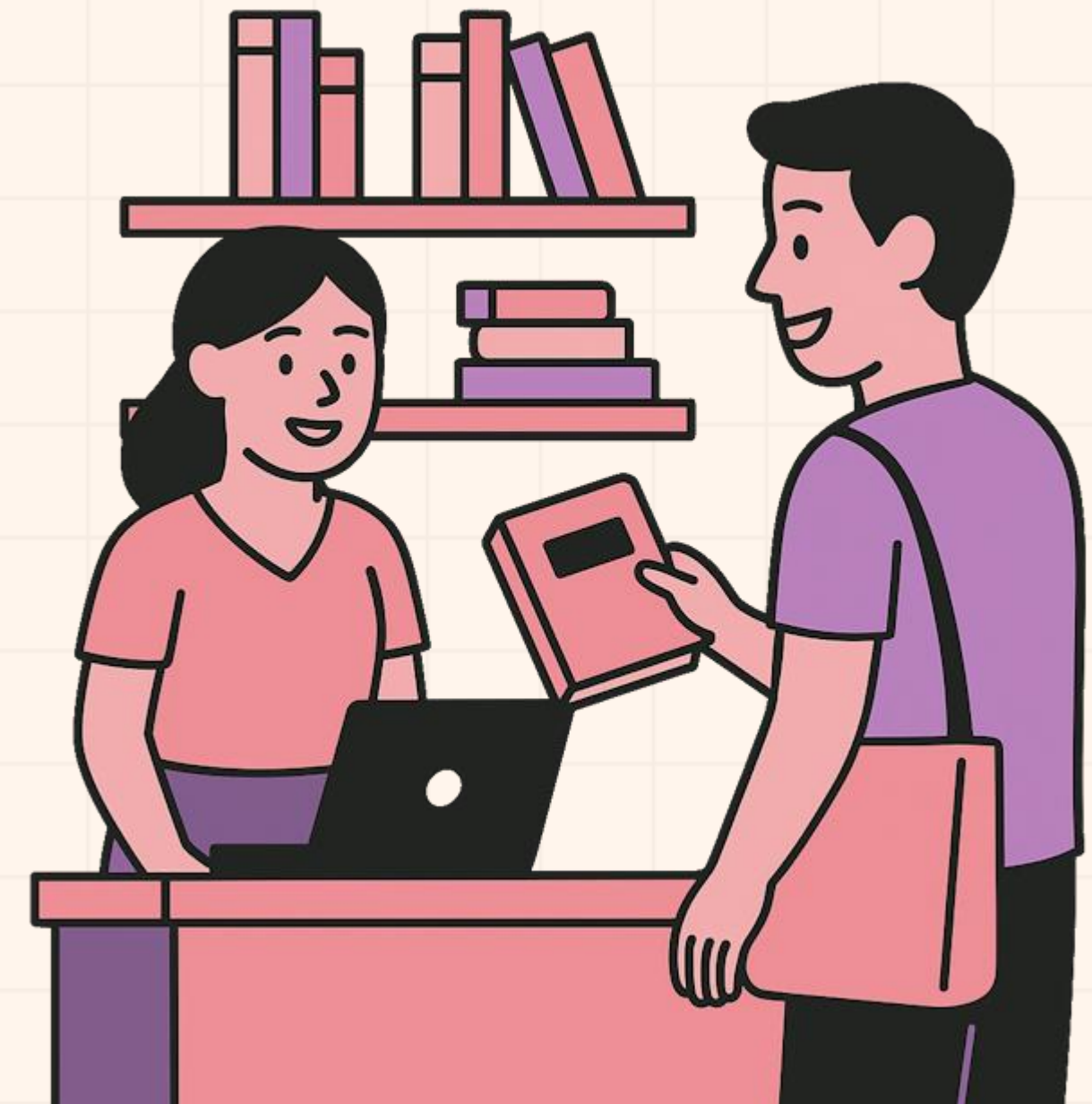
Awareness - True stories – Healthy Meal

- Someone posted a photo of healthy meal during COVID
 - Working remotely on in the usual business environment
 - Company laptop was in the background
 - Zoomed in and was possible to read emails
 - Company private information could be leaked
 - **Personal information of other persons was showing**
- Social Media Networks use OCR
 - Means they also read the emails
 - And everyone else on that social media could get the same information



Awareness - True stories – Store Credit

- Buying a book for almost no money
 - How I was able to get money just by having the right information
 - Store clerk asked for store customer card
 - Gave mobile number and full name
 - Store clerk asked if I wanted to use balance credit
 - I accepted and little had to pay
 - **Mobile number and full name were not mine**



Awareness - True stories - Customer Information (RGPD)

- Requesting invoice with NIF (not mine)
 - Invoice containing:
 - Name
 - Address (Shipping address)
- Adding store loyalty card with phone number
 - Invoice containing:
 - Name
 - Address (Shipping address)
- Updating someone's client data in store counter
 - Phone number
 - Email and address



OSINT

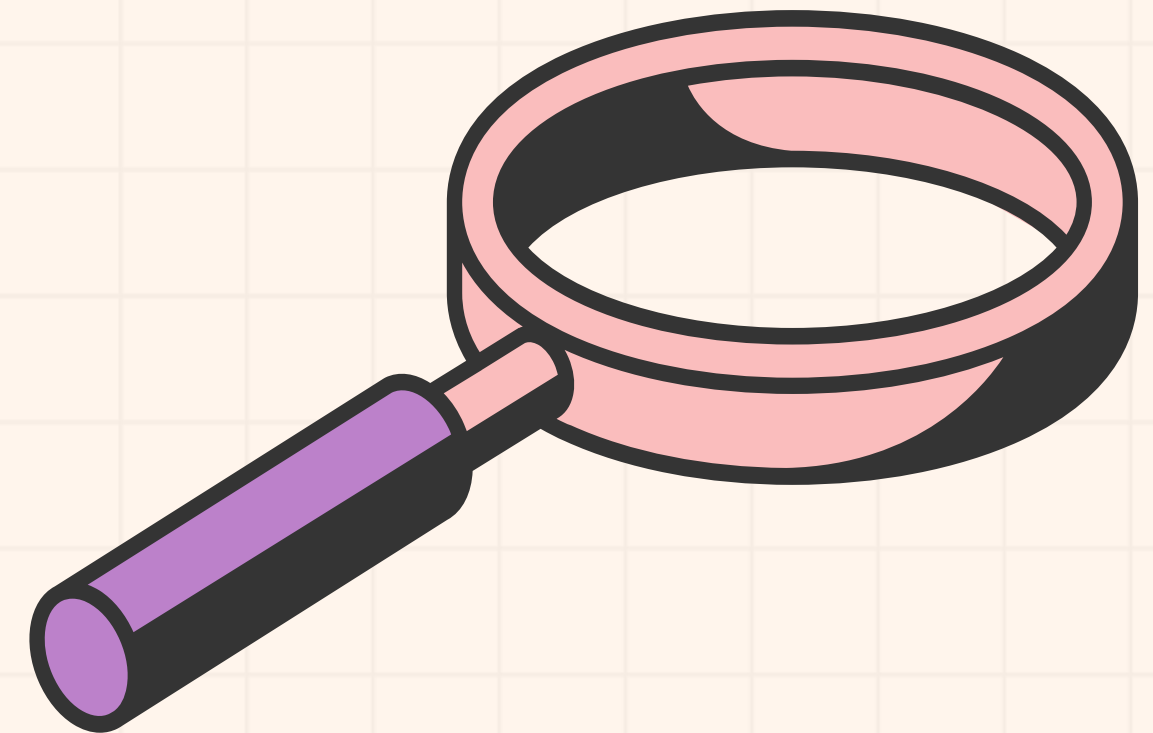


OSINT - Definition

Open-source intelligence (OSINT) is the collection and analysis of data gathered from open sources (overt and publicly available sources) to produce actionable intelligence. ([Wikipedia](#))

Gathering information from:

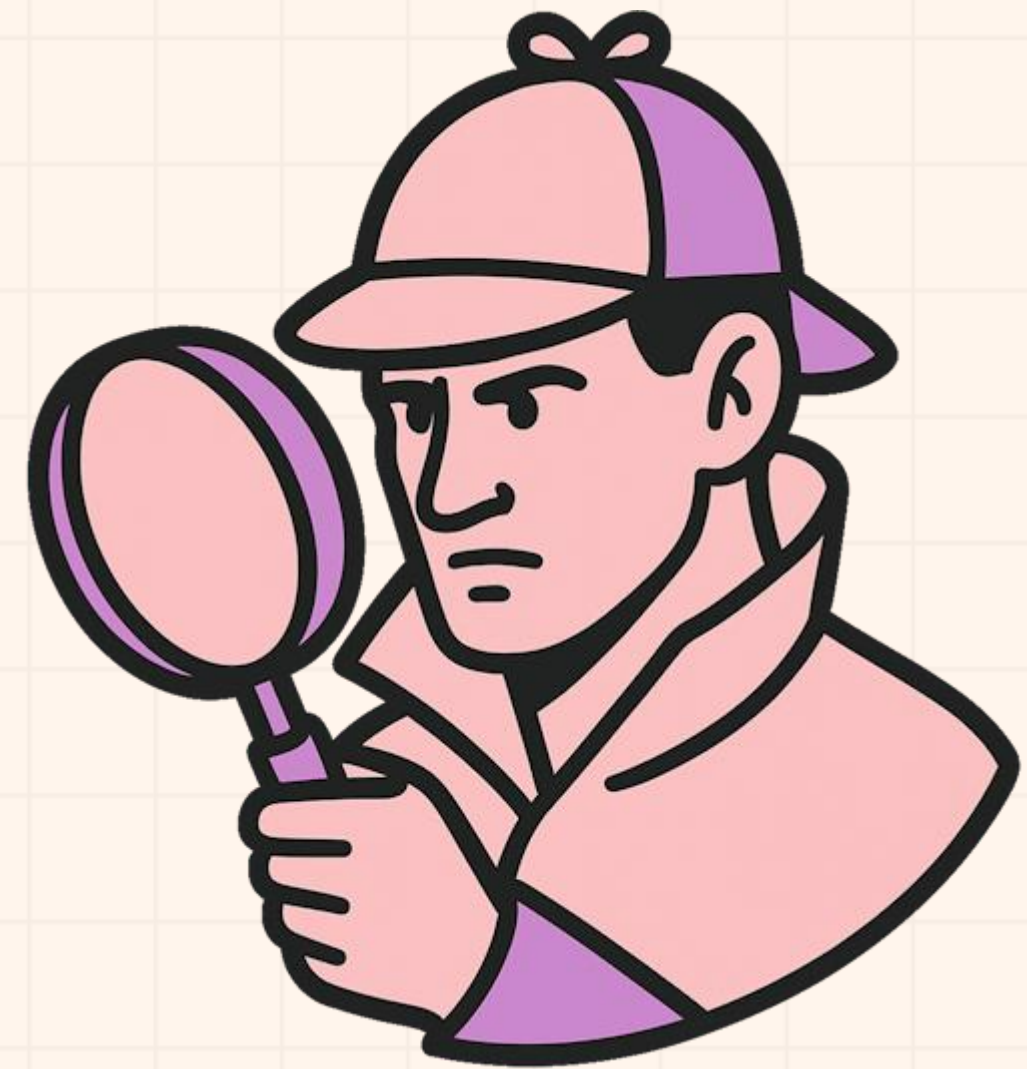
- government sites
- search engines (Google, ...)
- social media (Facebook, ...)
- maps
- ...



And then extract/relate/infer new information with greater value/potential

OSINT Time

“Information is not knowledge”
Albert Einstein



Who am I? – Let's OSINT me

- Starting with just a name
 - Pedro António Oliveira Vieira
- Google it ([link](#))
- Google “Improved Search” ([link](#))
- Google “Improved Search” + Company ([link](#))
- LinkedIn ([link](#))
 - Anonymous view (Just keep trying)
 - Public profile was showing way too much
- My GitHub notes ([link](#))
- Search, and then search again



Search Engines - Internet is more than Google

- Different search engine ➡ different rules/crawlers ➡ different results
- Google ([link](#))
- Bing ([link](#))
- DuckDuckGo ([link](#))
- Baidu (China) ([link](#))
- Yandex (Russia) ([link](#))
- SAPO (Portugal) ([link](#))



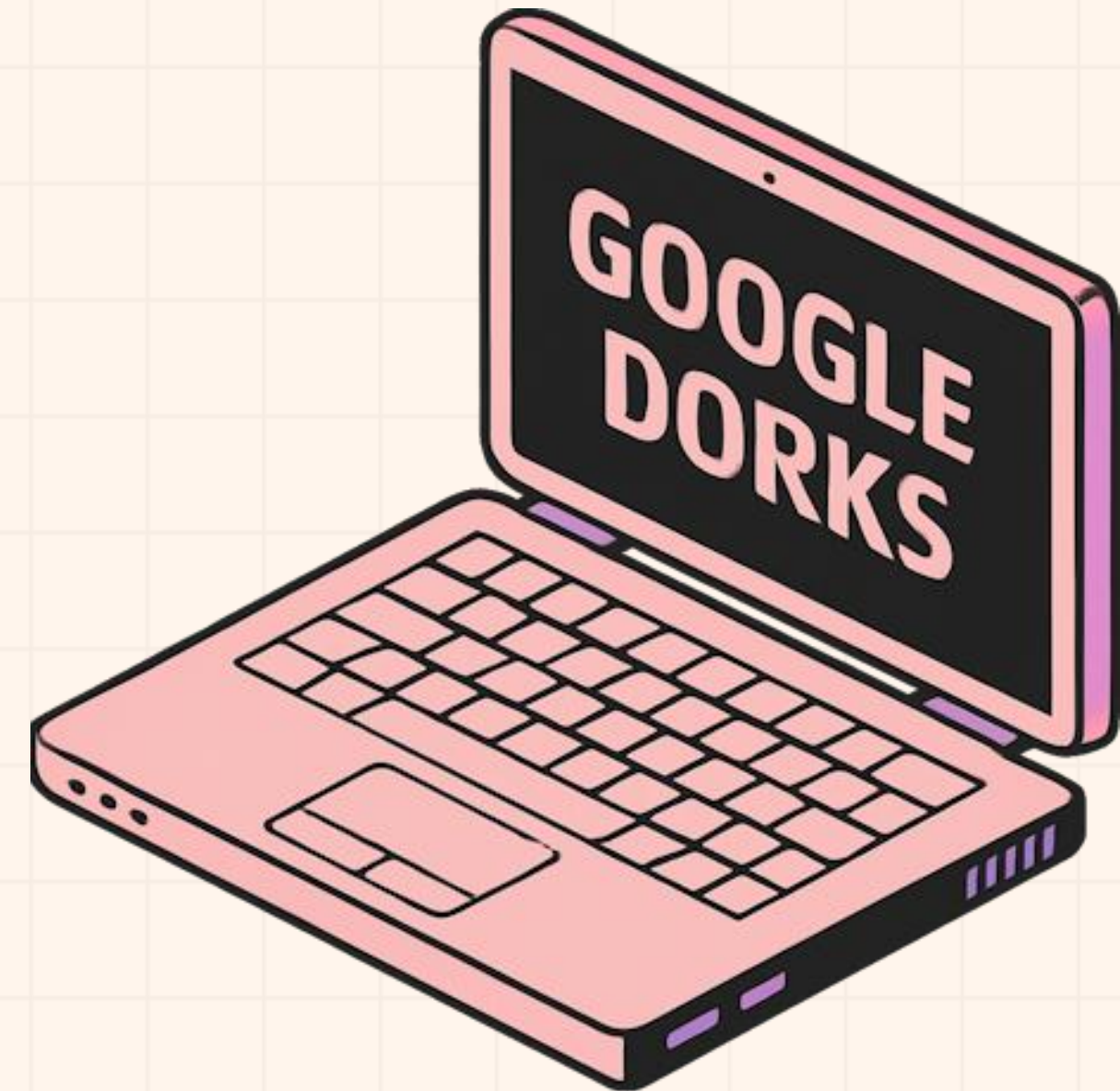
Improve the search - Search operators

- **filetype**: search your results based on the file extension
- **cache**: allows you to view cached version of the web page.
- **allinurl**: restricts results to pages containing all the query terms specified in the URL.
- **inurl**: restricts the results to pages containing the word specified in the URL
- **allintitle**: restricts results to pages containing all the query terms specified in the title.
- **link**: searches websites or pages that contain links to the specified website or page.
- **info**: finds information for the specified web page.
- **location**: finds information for a specific location.

- **42 Advanced Operators** ([link](#))

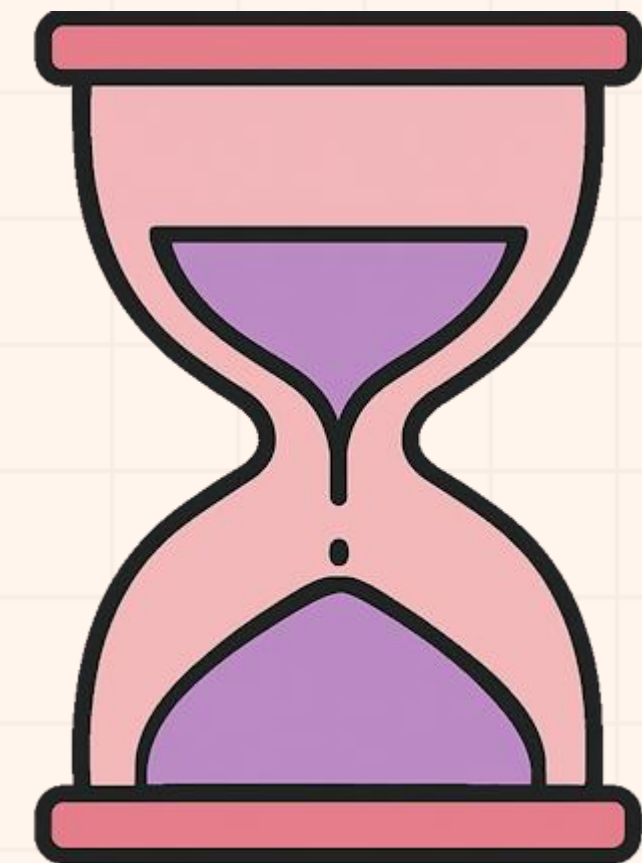
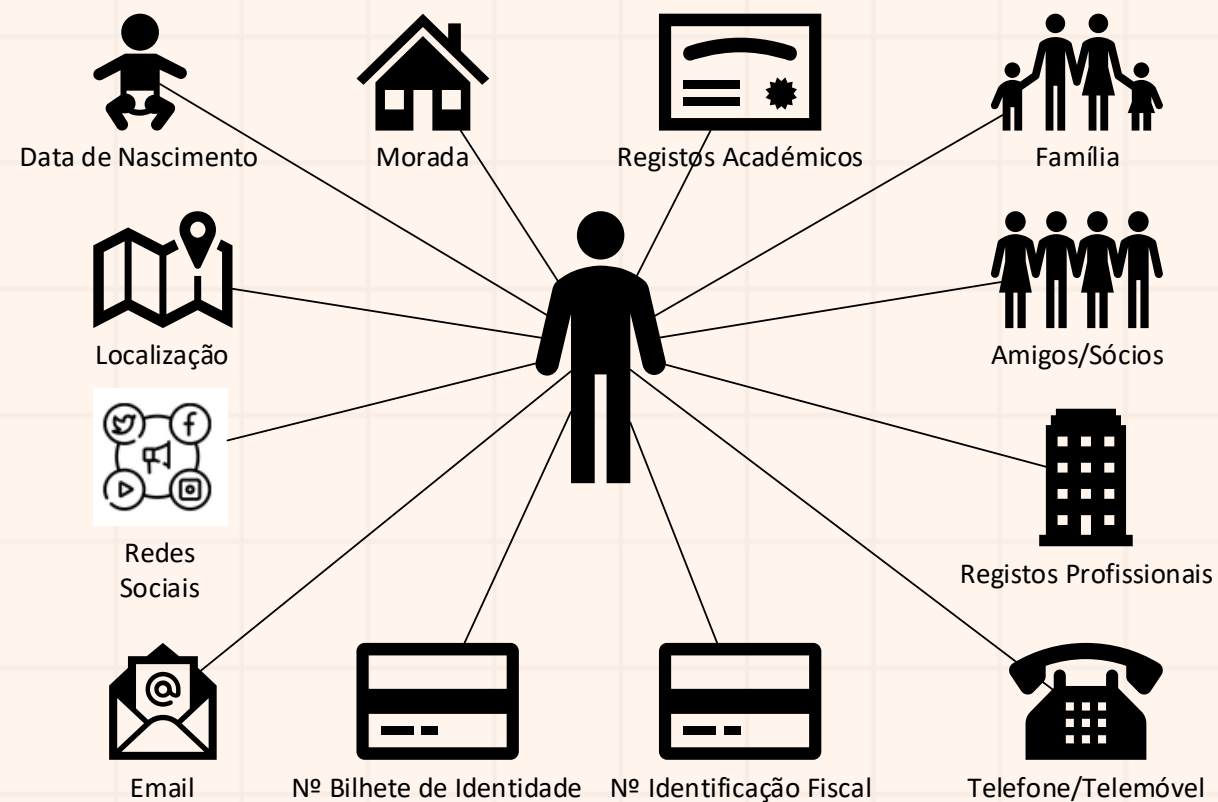
Improve the search - Google Dorks - Commonly used searches

- Google Advanced Search ([link](#))
- Google Hacking Database ([link](#))
- gbhackers ([link](#))
- google-dork-list ([link](#))
- Google Advanced Operators Guide ([link](#))



Who Are You? – Search yourself

- Search your name on Google and analyze the results
 - As you saw the search can be improved



EXERCISE TIME

- That is typically information to **verify your identity** over a phone call.



Who am I? – Let's OSINT me – AI version



What can you tell me about "Pedro Vieira". He is into cybersecurity and OSINT?

Pedro Vieira is a notable Portuguese cybersecurity professional with a strong focus on ethical hacking and open-source intelligence (OSINT).



Career Highlights

Top EC-Council Ethical Hacker: In January 2022, Pedro Vieira achieved the highest score globally on the EC-Council's Certified Ethical Hacker (C|EH) Practical exam, earning the prestigious C|EH Master credential.

Conference Speaker: Pedro was a featured speaker at RootedCON Portugal 2024, one of the country's leading cybersecurity conferences. His talk, titled "OSINT. Beware your data is out there," explored how publicly available information can be used to uncover sensitive data and highlighted the importance of privacy awareness.



OSINT Contributions

GitHub Repository: Pedro maintains a comprehensive GitHub repository dedicated to OSINT. This resource includes:

- Guides and notes on OSINT techniques
- Write-ups from platforms like TraceLabs and Hacktoria
- Training materials and curated tool lists
- Links to OSINT handbooks and educational videos



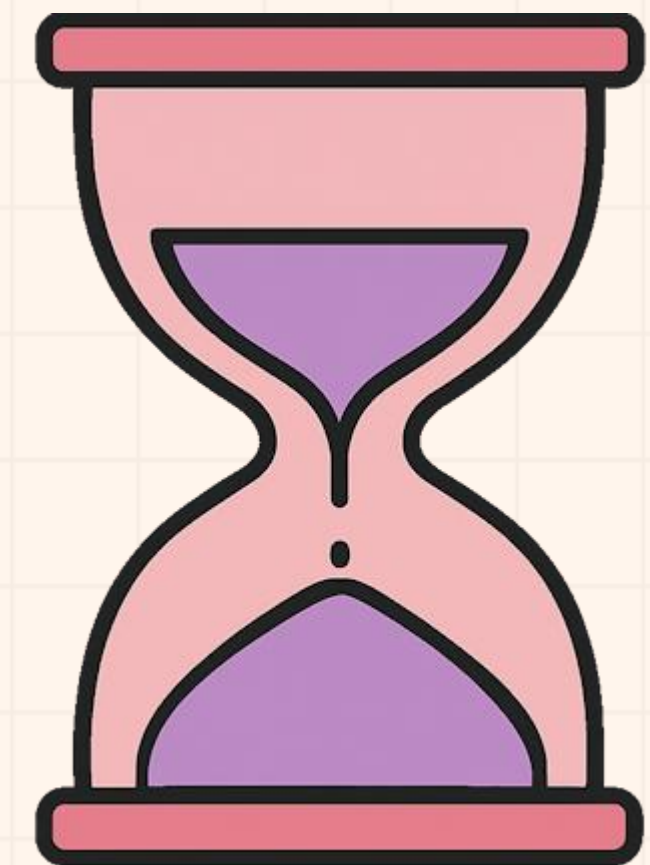
Professional Role

Cybersecurity Engineer at Bosch: Pedro has been serving as a cybersecurity engineer at Bosch Group in Braga, Portugal, since January 2020.

Improve the search or “Go lazy” – Go IA

- LLMs are like search engines on steroids
- **LLMS / Chatbots**
 - ChatGPT ([link](#))
 - Grok ([link](#))
 - Claude ([link](#))

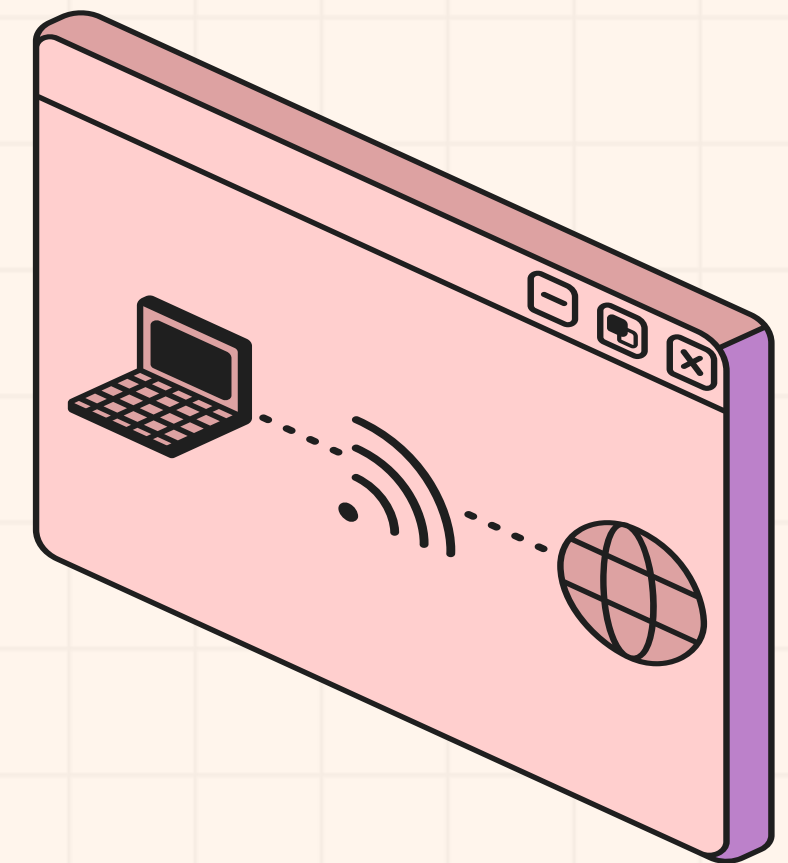
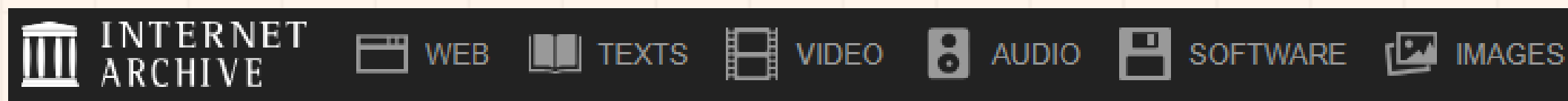
Models are bound by rules. They often don't provide personal information
Well, at least some commercial models



EXERCISE TIME

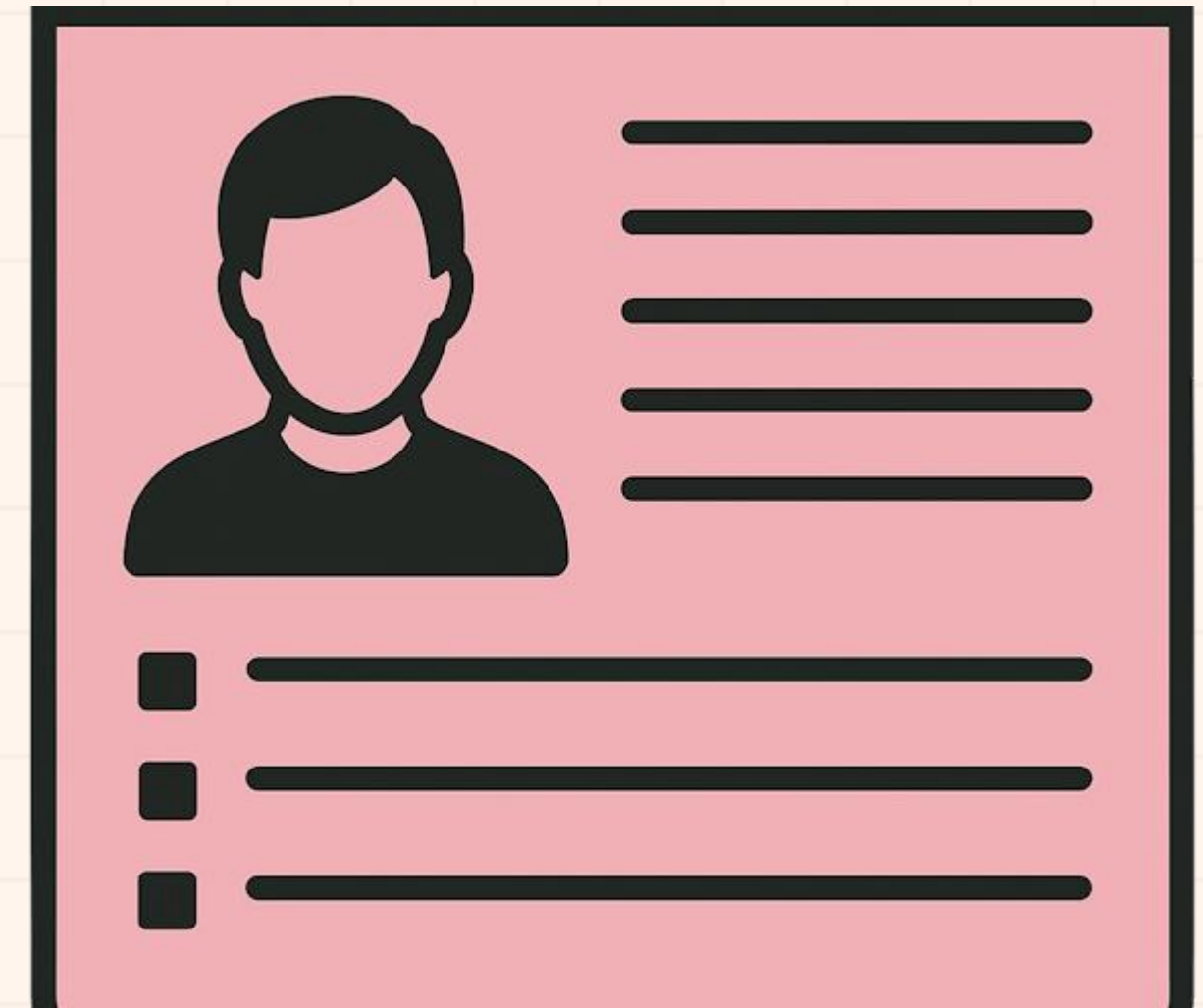
Search in the past - The internet knows and doesn't forget

- Posted information in private mode can be made publicly and world available by someone else
- When information is posted
 - Shows where you are at that time (habits & routines)
- The internet has memory
 - Arquivo.pt ([link](#))
 - Example ([link](#))
 - Internet Archive - Wayback Machine ([link](#))
 - Example ([link](#))



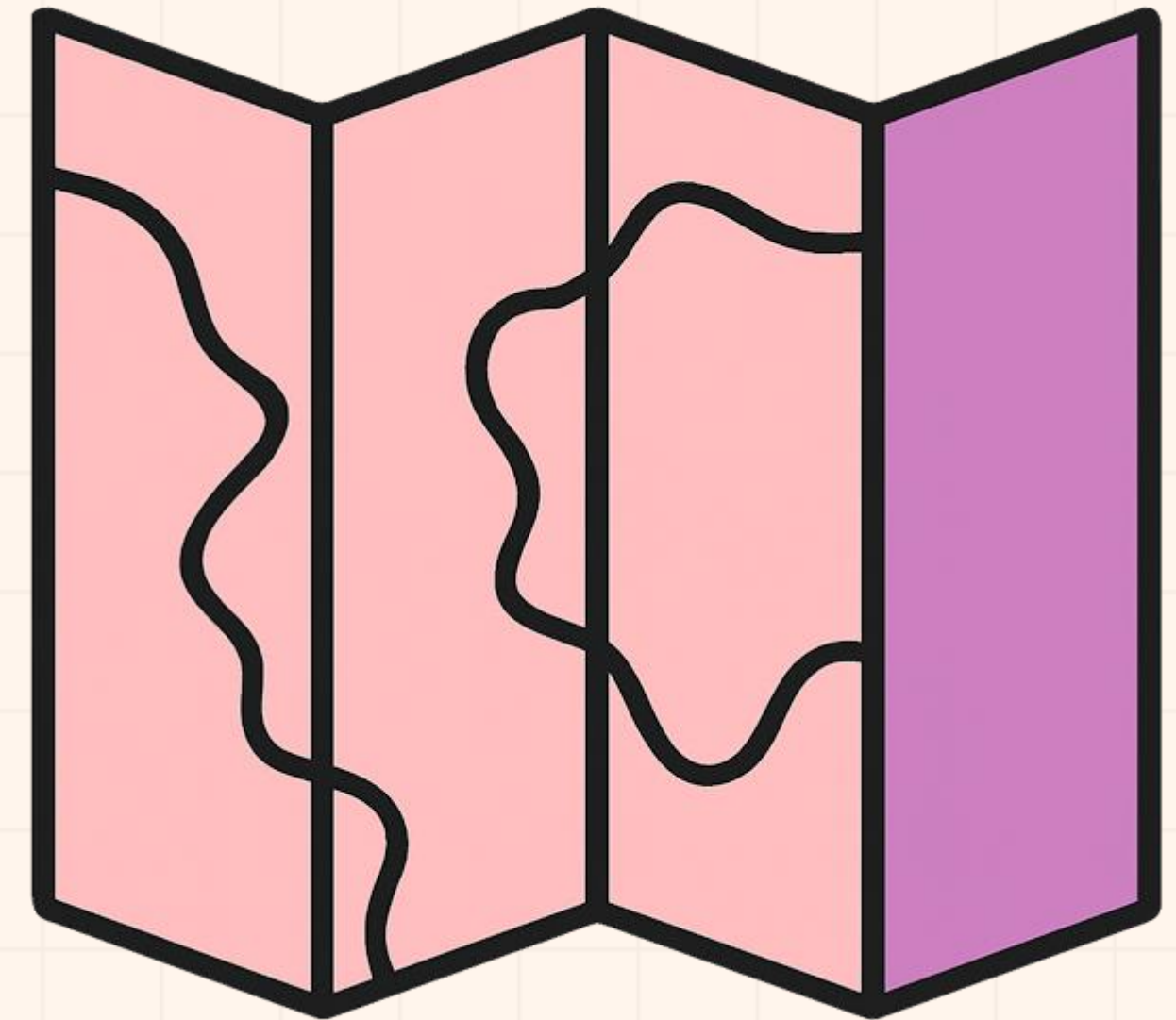
OSINT - Profile

- Phone number (Years using the same number)
 - Sync.Me ([link](#))
- Username
 - WhatsMyName ([link](#))
- Email (Username reuse)
 - Gmail ([link](#))
- Social Networks (Same username)
 - Facebook ([link](#))
 - LinkedIn ([link](#))
 - Tinder ([link](#)) ([link](#))
- If you don't have an account, I can create one and reach your friends.



OSINT - Maps

- Never been there. Know it like the back of my hand.
- Street view
 - Google Street View ([link](#))
- Map/ Satellite
 - Google Maps ([link](#))
 - Dual Maps ([link](#))
 - Overpass Turbo ([link](#))
 - Wizard: plant:source=nuclear
 - World Imagery Wayback example ([link](#))
- Tips, Tricks and Techniques ([link](#))



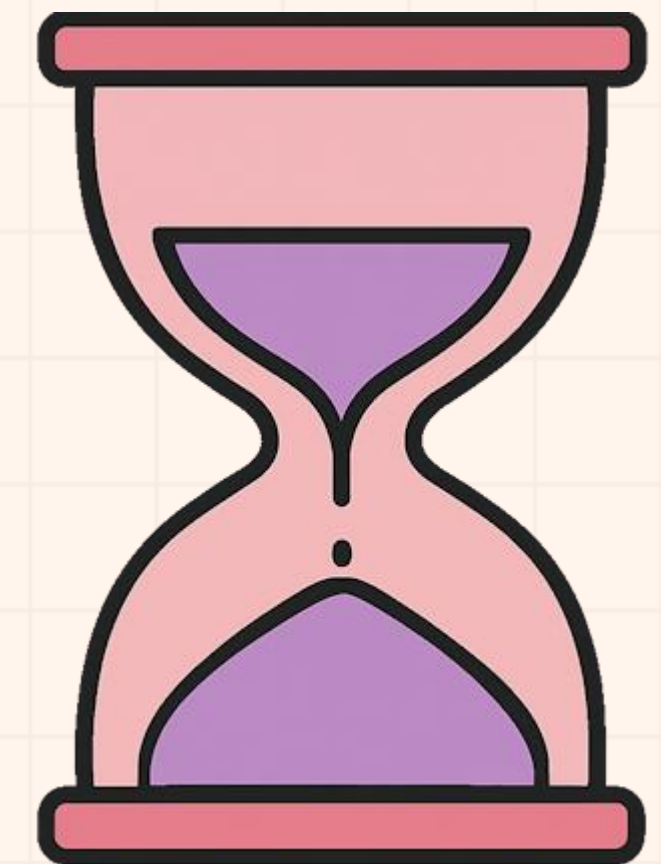
OSINT - Photos

- One image is worth 1000 words, maybe more.
 - What information can be extracted from a photo ?
- Photo analysis
 - Location ([link](#))
 - Date it was taken
 - Identifying elements in the photo
 - Boards
 - Signs
 - Flags
- The professionals (video explaining) ([link](#))



OSINT – Photos - Identify the location

- Where was this image taken?
 - Have you been there?
- When?
 - Date stamp on photo
 - Filename with date
 - Metadata
- What else?
- Image search
 - Identify the castle? ([link](#))



EXERCISE TIME


OSINT – Photos - Identify the location

- An image is worth a thousand words
- File analysis
 - Metadata
 - GPS ([link](#))
 - Google Maps ([link](#))
- Tools
 - CleanUp ([link](#))
 - AperiSolve ([link](#))

exifdata

SUMMARY
DETAILED
LOCATION
UPLOAD

IMG_20190223_163027.jpg



(click for original)

Camera
Xiaomi Redmi 3

GPS Position
40.989952 degrees N, 7.395051 degrees W

Date of Creation
2019:02:23 16:30:27

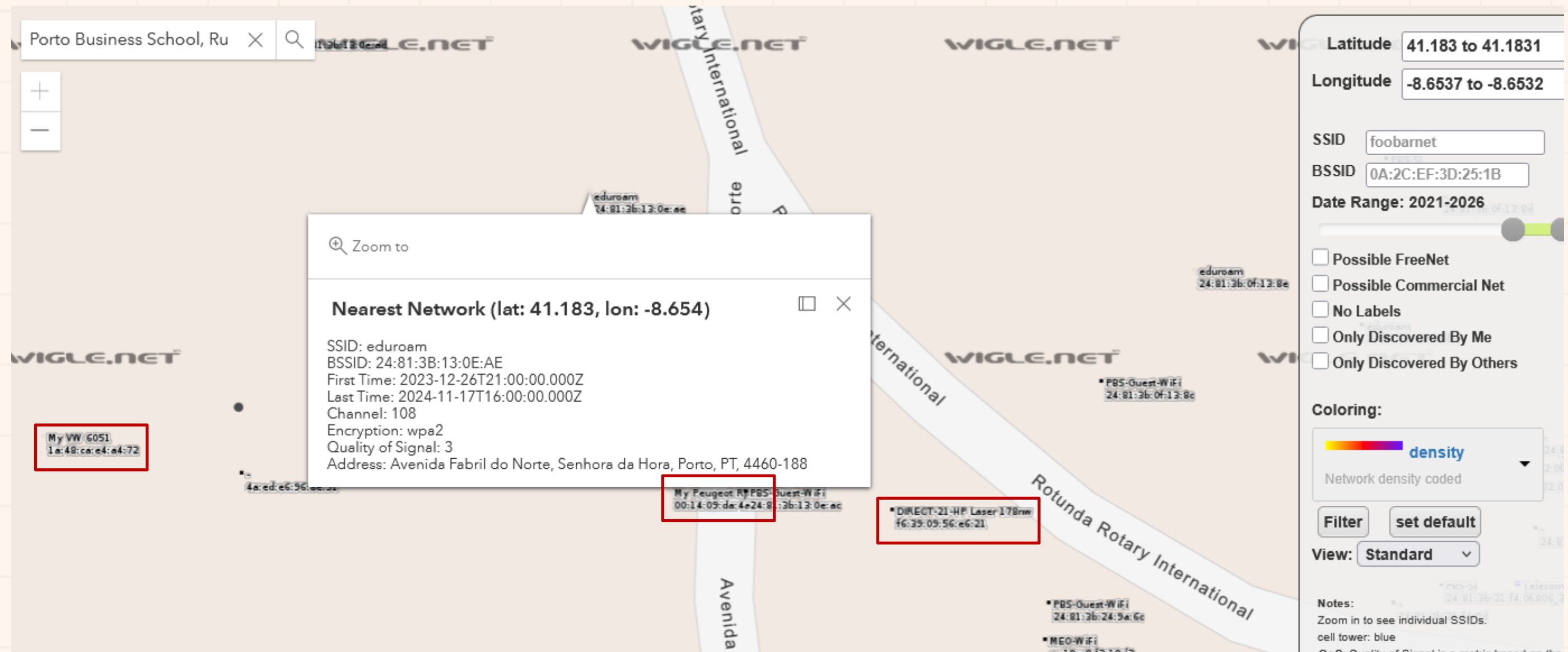
Resolution
4160x3120

SUMMARY

Make	Xiaomi
Model	Redmi 3
Aperture	2
Exposure Time	1/1506 (0.00066401062416999 sec)
Focal Length	4.2 mm
Flash	Auto, Did not fire
File Size	1447 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	4160
Image Height	3120
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered
Exposure Program	Not Defined
Date and Time (Original)	2019:02:23 16:30:27
Metering Mode	Center-weighted average
Color Space	sRGB
Exposure Index	140
Sensing Method	Unknown (0)
Exposure Mode	Auto
Focal Length In 35 mm	0 mm
Format	
Scene Capture Type	Standard
Gain Control	Low gain up
ISO	100
Compression	JPEG (old-style)

OSINT - World Map - WiFi Networks

- Wiggle ([link](#))
- Routers
- Printers
- Cars
- IoT
- ...



OSINT - World Map - WiFi Networks

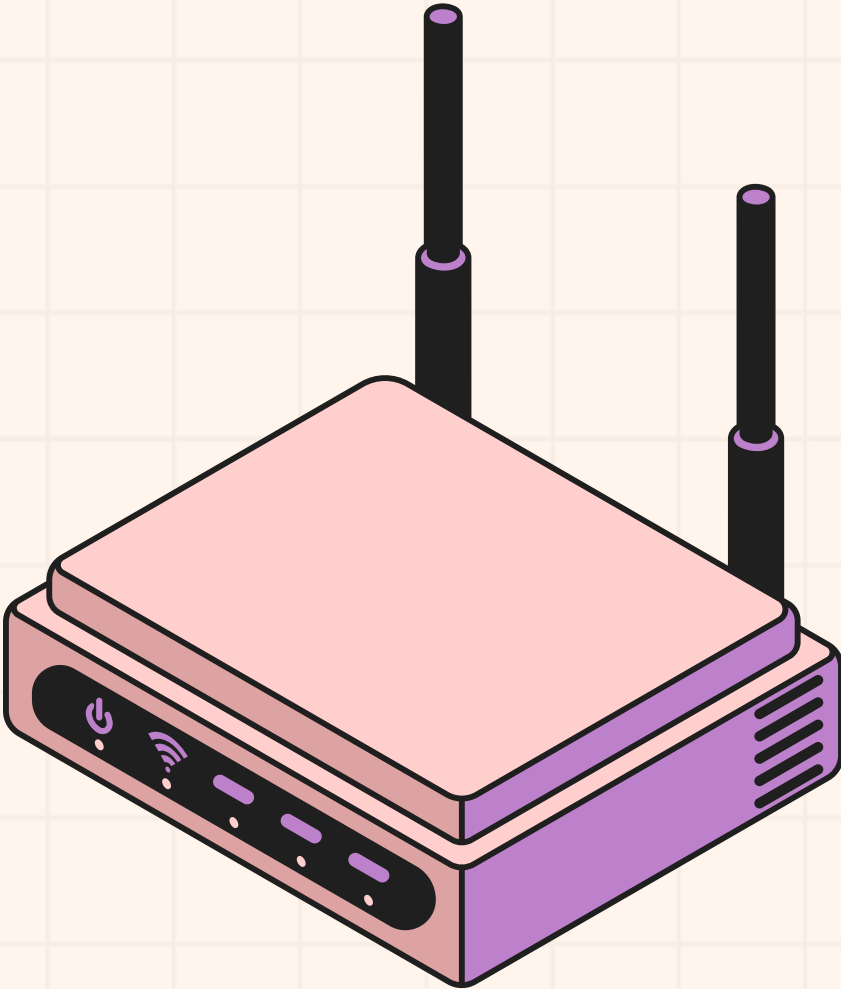
- Wiggle ([link](#))

🔍 Zoom to

Nearest Network (lat: 41.183, lon: -8.654)

SSID: eduroam
BSSID: 24:81:3B:13:0E:AE
First Time: 2023-12-26T21:00:00.000Z
Last Time: 2024-11-17T16:00:00.000Z
Channel: 108
Encryption: wpa2
Quality of Signal: 3
Address: Avenida Fabril do Norte, Senhora da Hora, Porto, PT, 4460-188

The MAC address "c0:25:5c:49:A5:3A" has been assigned by the IEEE to:	
MAC-Segment:	C0:25:5C:00:00:00 - C0:25:5C:FF:FF:FF (MA-L)
Vendor:	Cisco Systems, Inc
Address:	170 West Tasman Drive San Jose CA 95134 US




OSINT - Companies

Demo Time

Porto Business School

- Porto Business School ([link](#))
- Google - Search PBS NIF ([link](#))
 - 508541832

Portal



IMT - Instituto da Mobilidade e dos Transportes

- CAE ([link](#))
- CAE Principal – 85400 – Ensino Superior
- 35123 - Produção de eletricidade de origem solar
- 70200 - Atividades de consultoria ...

Portal



Ministério da Justiça – Publicação de Atos Societários

Data	Entidade	Concelho	Acto/Facto	Conteúdo	Documento	
2015-04-29	Associação EGP - U. Porto	Matosinhos	Alteração de Estatutos de Associação	Conteúdo	Documento	
2015-03-23	ASSOCIAÇÃO EGP – U. PORTO	Matosinhos	Alteração de Estatutos de Associação	Conteúdo	Documento	
2014-02-11	ASSOCIAÇÃO EGP – U. PORTO	Matosinhos	Alteração de Estatutos de Associação	Conteúdo	Documento	
2012-07-12	ASSOCIAÇÃO EGP - U. PORTO	Porto	Rectificação de Associação	Conteúdo	Documento	
2012-06-25	ASSOCIAÇÃO EGP-U.PORTO	Porto	Alteração de Estatutos de Associação	Conteúdo	Documento	
2011-07-07	ASSOCIAÇÃO EGP-U.PORTO	Porto	Alteração de Estatutos de Associação	Conteúdo	Documento	
2008-06-11	EGP - UNIVERSITY OF PORTO BUSINESS SCHOOL, ASSOCIAÇÃO	Porto	Constituição de Associação	Conteúdo	Documento	

OSINT - Companies

Demo Time



base:
CONTRATOS PÚBLICOS ONLINE

Portal BASE

www.base.gov.pt

- Entity ([link](#))
- Contracts ([link](#))

[Início](#) / [Detalhe](#)

Última atualização: 28 abr.2023

DETALHE
Entidade

IMPRIMIR DETALHE

Informação detalhada

NIPC	508541832
Descrição	Porto Business School
Localização da sede	Portugal
Nº de contratos como adjudicante	11
Total gasto	10.945.195,94 €
Contratos como adjudicante	Lista dos contratos
Nº de contratos como adjudicatária	70
Total ganho	2.189.901,78 €
Contratos como adjudicatária	Lista dos contratos

OSINT - Companies

Relatórios de Empresas ▾

Softwares com Dados ▾

Licenciamento de Dados ▾

Estudos de Mercado ▾

+ ▾

Posição: Home Relatórios de Empresas ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U.PORTO

508541832 contribuinte de ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U.PORTO

Esta empresa foi consultada **346** vezes nos últimos 12 meses, a última vez a **17 de maio de 2025**.

NIF: 508541832

DUNS: 337576166

Denominação: ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U.PORTO

Designações anteriores: ASSOCIAÇÃO EGP - U.PORTO

EGP - UNIVERSITY OF PORTO BUSINESS SCHOOL

Morada: AVENIDA FABRIL DO NORTE, 425

Código Postal: 4460-312 SENHORA DA HORA

Atividade (CAE): 85400 - Ensino superior

Antiguidade: 16 ano(s)

Telefone: 226153...

Email: ...@pbs.up.pt

Website: pbs.up.pt

Balanço disponível: NÃO

Acesso ao serviço:

Email

Password

Entrar

Esqueceu-se da sua password de acesso?

Registe-se e aceda ao relatório desta empresa

Exemplo>

O que inclui o relatório?

- Semáforo do Risco de Failure
- Evolução das Vendas e Resultados (3 anos)
- NIF, Nome, Contactos e Atividade da empresa

Associação Porto Business School (pbs) - U. Porto

ATIVA

Partilhar

Dados Gerais

Resumo

Rácios Financeiros

Evolução

Estrutura Corporativa

Atos Societários

Alguns dados errados nesta empresa?

Dados Gerais de ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U. PORTO

DATA DE ÚLTIMA CONSULTA

18 maio 2025

RAZÃO SOCIAL

ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U. PORTO

DENOMINAÇÃO COMERCIAL

ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U. PORTO

NIF DE ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U. PORTO

508541832

FORMA JURÍDICA

Associação

MORADA DE ASSOCIAÇÃO PORTO BUSINESS SCHOOL (PBS) - U. PORTO

Av. Fabril Do Norte Nr. 425 4460-312 - SENHORA DA HORA. PORTUGAL

CÓDIGO POSTAL

4460-312 - SENHORA DA HORA

CONCELHO

Senhora Da Hora

DISTRITO

Porto

WEBSITE

www.pbs.up.pt

CAE

85400 - Ensino superior

SETOR DA EMPRESA

Ensino Superior

INCIDENTES JUDICIAIS

Aceder

ALERTAS DE ALTERAÇÕES RELEVANTES

Aceder

DATA DE CONSTITUIÇÃO

2008/06/05

Volume de negócios

€

Capital social

€

Evolução volume de negócios

Dimensão da empresa

Empregados

Resumo de Associação Porto Business School (pbs) - U. Porto


A sociedade Associação Porto Business School (pbs) - U. Porto está localizada no concelho de Senhora Da Hora, situada no distrito de Porto, com o código postal 4460-312 - Senhora Da Hora. A sociedade está devidamente inscrita na Conservatória do Registo Comercial do distrito de Porto.

Seguindo a classificação do CAE, Associação Porto Business School (pbs) - U. Porto dedica-se à atividade classificada como Ensino Superior. Mais especificamente, a sua categoria é identificada como Ensino Superior, com o código numérico correspondente 85400.

O NIF de Associação Porto Business School (pbs) - U. Porto é 508541832, e a sua

Page 32

OSINT - Companies



Pesquisar Empresas









Estado

Em Atividade (1)

Localização

Porto (1)

4 resultados

		Localização	Ordenar por >
	Associação Egp - U. Porto NIF: 508541832	 Porto	>
	Leadership Grand Conference NIF: 508541832	 Portugal	>
	Leadership Grand Conference NIF: 508541832	 Portugal	>
	Porto Business School NIF: 508541832	 Portugal	>

OSINT - Companies

The screenshot displays the Hunter.io web application interface. On the left is a sidebar with navigation links: Dashboard, Discover, Finder (highlighted), Verifier, Bulks, Signals, Leads, Campaigns, Integrations, and API. At the bottom of the sidebar are Notifications (1) and Support.

The main content area features a search bar with two tabs: "Find email by company" (selected) and "Find email by name". Below the search bar is a "Domain Search" section where "pbs.up.pt" has been entered. To the right of the search bar, it shows "pbs.up.pt 41 results" and a search icon.

Below the search bar, a box indicates "41 results for pbs.up.pt". Underneath this, there are filters for "Type", "Department", "Job title", and "Show only results with". Below the filters, there are two tabs: "All people" (selected) and "Decision Makers".


The results are categorized by department. Under "IT / Engineering (1)", there are no results shown. Under "Management (2)", two results are listed:



- Carlos V.**
*****@pbs.up.pt
Manager (with LinkedIn icon)
- Susana O.**
*****@pbs.up.pt
Manager (with LinkedIn icon)

Each result has a "Reveal email address" button with a lock icon and the number "1".


On the right side of the interface, there is a notification box for "Universidade do Porto" with a "Follow this company" button. Below this is a "Company" section for "Universidade do Porto", which includes a description: "Universidade do Porto is a Higher Education institution that offers academic programs and conducts research." and a "Accept all: NO" button.

OSINT - Vehicles

Portal	Automóvel On-line
 <p>Automóvel On-line www.automovelonline.mj.pt</p>	<ul style="list-style-type: none"> Certidão Permanente do Registo Automóvel (link) <ul style="list-style-type: none"> Document example (link) Demo: search for a car (link) <ul style="list-style-type: none"> License Plate : 89-QS-04 (link)

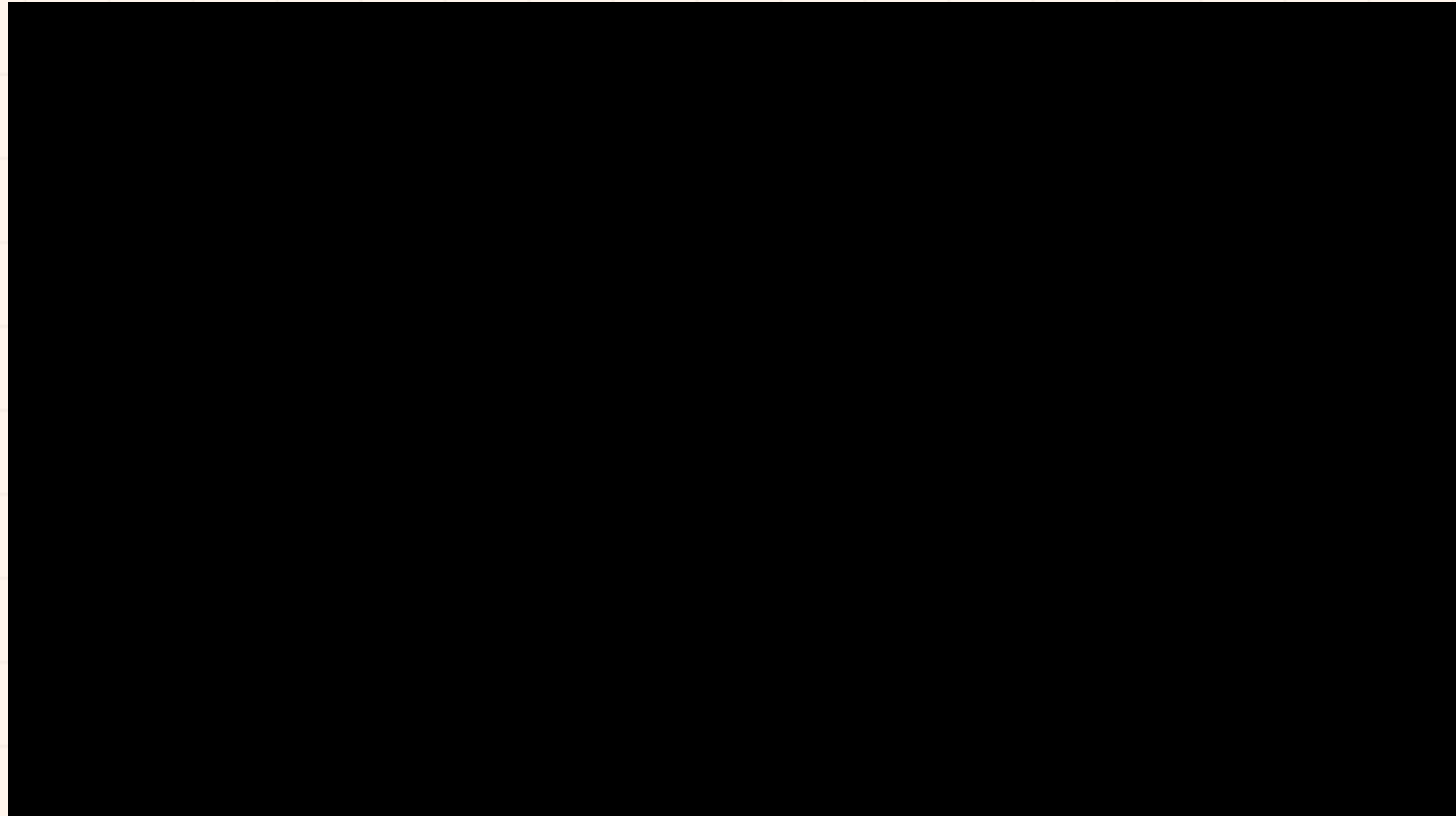
Portal	IMT - Instituto da Mobilidade e dos Transportes
 <p>Instituto da Mobilidade e dos Transportes www.imtonline.pt</p>	<ul style="list-style-type: none"> Serviços IMT online.pt (link)  Veículos → Certidão <ul style="list-style-type: none"> Mandatory inspection Vehicle characteristics

Portal	ASF – Autoridade de Supervisão de Seguros e Fundos de Pensões
 <p>ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões www.consumidor.asf.com.pt</p>	<ul style="list-style-type: none"> Check Insurance (link) License Plate : 89-QS-04

Portal	Lastvin
 <p>LastVIN.com www.lastvin.com</p>	<ul style="list-style-type: none"> Mercedes-Benz VIN Decoder (link) Will the prime-minister keep the car?

Hack across the globe by VIN ([link](#))

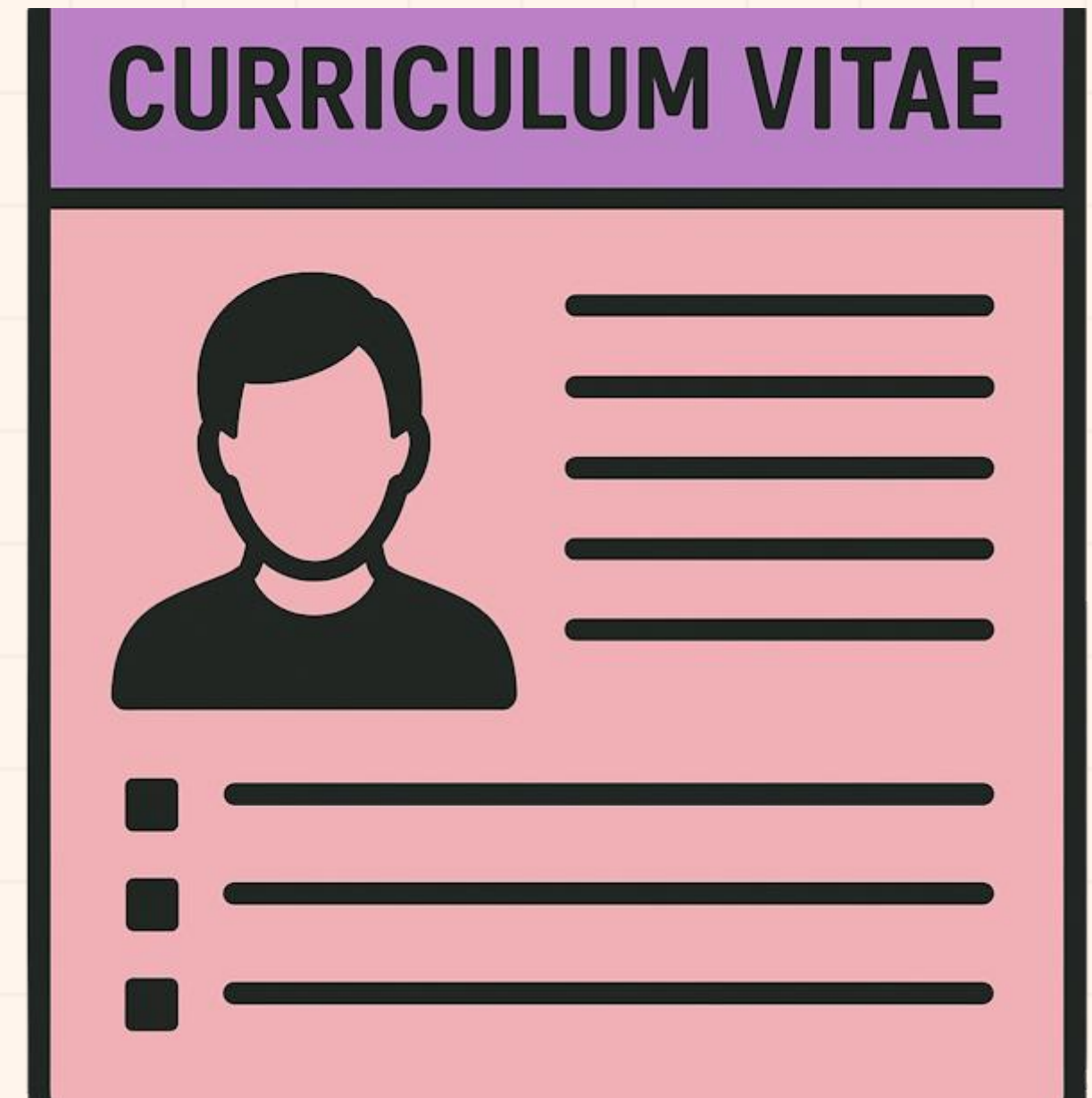
AITI – Brunei Darussalam





Internet Search - Curriculum Vitae

- Google Search
 - "curriculum vitae" filetype:pdf site:.pt ([link](#))
 - "curriculum vitae" filetype:pdf inurl:upload ([link](#))
- Curriculum Vitae
 - Sending CV with too much information – what is too much
 - Home address – Street View
- Professional information phishing
 - Fake job adds (Is this a thing?)



Internet Search - Pay slip

- Don't open links just because they are available.
 - It's like entering a house just because the door was open. Would you do that ?
- Google Search ([link](#))
- Bing Search ([link](#))
- Yahoo Search ([link](#))
- “recibo de vencimiento” filetype:pdf
 - “recibo de vencimiento” – keywords to look for
 - filetype:pdf - only pdf files
- Available information on pay slips
 - Full name, address, nif, nib, marital status, number of children, ...



Internet Search - Hacked Websites

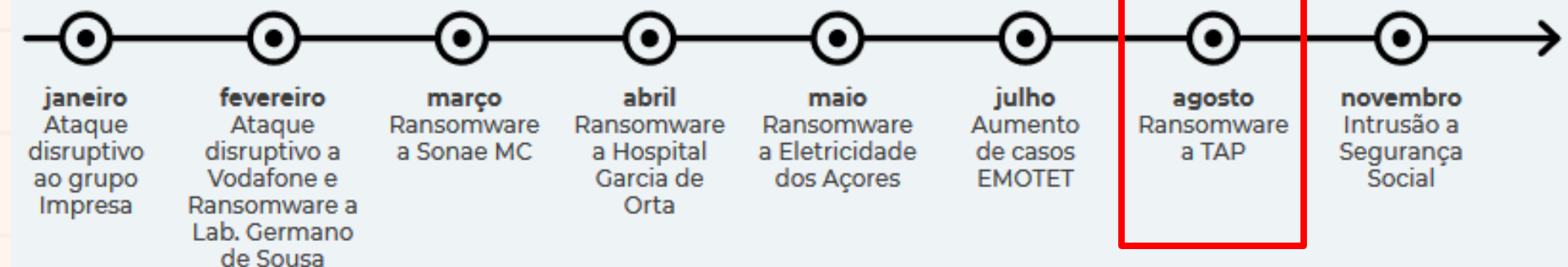
- Google Search ([link](#))
- allintitle:"hacked by" site:pt
 - "hacked by" - keyword to look for
 - site:pt - only "portuguese" sites (registered portuguese domains)
- About 6.200 results
 - Sites / pages that were "tagged"/"signed"
 - Attack and contents changed to show off skills (mainly kids)
 - compared to street tagging



Data breach - When companies are hacked

- When companies are hacked, private data is exposed. Private data becomes “public”. ([link](#))
- Troy Hunt
 - HavelBeenPwned ([link](#))
 - Pwned websites ([link](#))
 - Domain search ([link](#))
- CNCS Report
 - Cybersecurity in Portugal 2024 ([link](#))
 - Cybersecurity in Portugal 2023 ([link](#))

CRONOLOGIA DE ATAQUES NO CIBERESPAÇO COM IMPACTO ELEVADO EM PORTUGAL, 2022*



*Consideram-se como ataques no ciberespaço com impacto elevado os incidentes com efeitos relevantes nos serviços e infraestruturas e/ou com visibilidade social, cuja investigação já tenha revelado conclusões suficientes para serem descritos

Fonte: CNCS

Data breach - Credentials

- Source
 - “Publicly” available list of credentials
- Information gathered
 - Rule of email/login
 - Rule of password complexity
 - List of users
 - Phishing campaigns
 - Brute force
- Look for those users on Social Media
 - Reuse of credentials

```

data/m/b:mlfer#15
data/m/c:mc:boris2249
data/m/c:mc:cunha1
data/m/c:mc:mcunha
data/m/j:mj:ca.pt:1107mj
data/m/s:ms:pt:MilanKundera
data/m/s:ms:pt:10222406
data/m/t:mt:pt:21646695
data/p/a:pa:pt:9023lqpg
data/p/a:pa:pt:ciqewyda
data/p/g:pg:ca.pt:9023lqpg
data/p/g:pg:ca.pt:Gon
data/p/g:pg:ca.pt:mypetige
data/p/l:pl:ca.pt:brandol
data/p/l:pl:ca.pt:qlindo01
data/p/l:pl:ca.pt:nfv02VDK
data/p/n:pr:ca:dyhanoge
data/p/t:pt:pt:fbobh_$g%1
data/p/t:pt:pt:nokupeku
data/p/t:pt:pt:recoreco
data/p/t:pt:ca.pt:Pteixeira
data/p/t:pt:ca.pt:kyawee
data/p/t:pt:ca.pt:teixeira10
data/p/t:pt:ca.pt:xocuwuti
data/r/a:ra:pt:99999999
data/r/a:ra:pt:fbobh_s371
data/r/a:ra:pt:sytaruru
data/r/m:rm:pt:zabolegy
data/s/c:sc:ca:advogada
data/s/d:sd:ca.pt:tsunami1
data/s/e:se:ca:4nick8nela
data/s/e:se:ca:awyixk
data/s/g:sg:ca.pt:snfg1500
data/s/i:si:ca:diogofofo
data/s/m:sm:ca.pt:monteirodasilva
data/s/m:sm:ca.pt:silvamonteiro
data/s/o:so:ca:capricornio
data/s/u:su:ca:mametiry

```


Data breach – Credentials - Portuguese domain examples (2018)

- uminho.pt - Universidade do Minho
- adv.oa.pt - Ordem dos Advogados
- pj.pt - Policia Judiciária
- mail.exercito.pt - Exército
- cm-braga.pt - Câmara Municipal de Braga
- cm-guimaraes.pt - Câmara Municipal de Guimarães
- psd.pt - Partido Social Democrata
- ps.pt - Partido Socialista
- fcporto.pt - Futebol Clube do Porto
- min.justiça - Ministério da Justiça

IOT Search engines

- Shared folders accessible to 8 thousand million people ([link](#))

- Contabilidade – 6
- Clientes – 3
- Faturacao – 1
- Primavera – 6
- SAGE – 13
- Winrest – 148

Shares			Shares		
Name	Type	Comments	Name	Type	Comments
Web	Shares		ADMIN\$	Disk	Remote Admin
Public	Name	Type	C\$	Disk	Default Share
homes			IPC\$		
SCAN	Multimedia	Shares	Printer		
SERVER	Download	Name			
Multimedia	Web				
Recordings	Public	Multimedia			
home	homes	Download			
MBPT	TESTE	Web			
PLOUTOS	JOAO	Public			
TGS	DUDA	homes			
MIRUS	SEGMENTO_POPULAR	BackupR			
USB	SOFTWARE	home			
IPC\$	home	IPC\$			
	IPC\$				

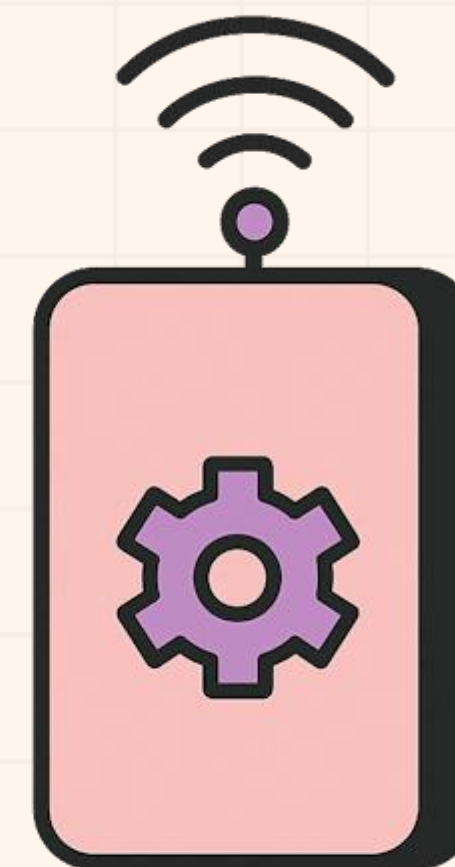
Shares		
Name	Type	Comments
IPC\$	IPC	IPC Service ("")
Carlos	Disk	Carlos Pessoal
TTT	Disk	Todo Tipo Terre
SAIG	Disk	SAIG
Zonesoft	Disk	Clientes Zoneso
FTP	Disk	FTP
Clientes_Sage	Disk	Clientes Sage
Clientes_XD	Disk	Clientes XD
XD Extreme	Disk	XD Extreme
video	Disk	System default
photo	Disk	System default
music	Disk	System default
admin	Disk	...

Message from Ella

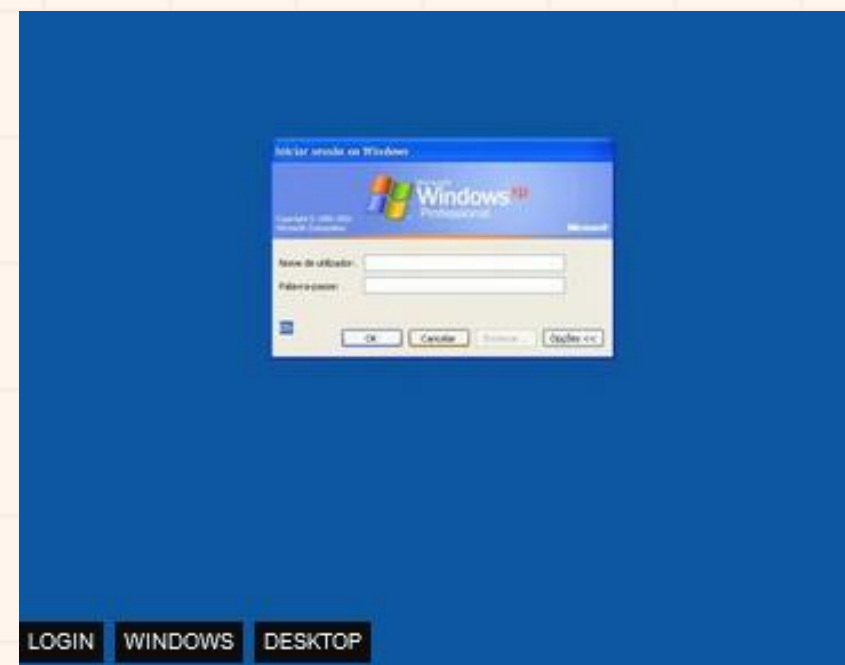


Internet of Things

IoT



OSINT - Shodan – IoT Search Engine



OSINT - Shodan – IoT Search Engine

Shodan Maps Images Monitor Developer More...

SHODAN Images |screenshot.label:ICS country:pt

// FOUND 2 RESULTS

WinRest FrontOffice POS

17:32 MOUNT SAINT CHARLES ACADEMY PLANT MASTER 06/29/22

82°

SCHOOL STEAM 0.0 #

PLANT ALARM

ALARM SILENCE

AT A GLANCE

0.2 #

1

2

CONTROL ALARM

CONTROL ALARM

SCREEN ICS

MCR Fred and George Pump Station

76.1 F

00:04:14 01 JUL 22

Tank Level 14.92 Ft

2 - Alarm Panel

3 - Operating

4 - Graph

5 - Unit Pressures

0 RPM

11 Psig

926 RPM

1619 Psig

0 RPM

14 Psig

ICS POS 12

TOWN OF EDMESTON WATER SYSTEM

VALVE CONTROL

High Alarm: 9.5 FT

Stop Fill: 9.3 FT

Start Fill: 8.3 FT

Low Alarm: 7.8 FT

RESERVOIR

8.54 FEET

Current Day: 60638 GAL

Previous Day: 88650 GAL

Flow Meter: 60638 GAL

Preset: 0 GAL

CL2 RESIDUAL: 1.54 PPM

CL2 RESIDUAL: 0.00 PPM

AC POWER

BATTERY

ICS POS

HYDROFLUX industrial WASTE WATER TREATMENT PLANT

5:34:47 AM 7/1/2022

SBR MIMIC

TRENDS

SETPOINTS

NO ACTIVE ALARMS

FAULT RESET

LOGIN

GUEST

ICS POS

OSINT - Shodan – IoT Search Engine

- Internet Exposure Observatory
 - Exposure Dashboard ([link](#))
- Explore
 - Shodan explore ([link](#))
- Images
 - Shodan images ([link](#))
- Maps
 - Shodan maps ([link](#))
- Remote Desktop ([link](#))
 - Total results: 2,745,593
 - Braga ([link](#))
- Imagens
 - Braga ([link](#))
 - VNC Remote Access and Loggedin ([link](#))
- Authentication Disabled
 - Portugal ([link](#))
 - Fotos ([link](#))
 - Contabilidade ([link](#))

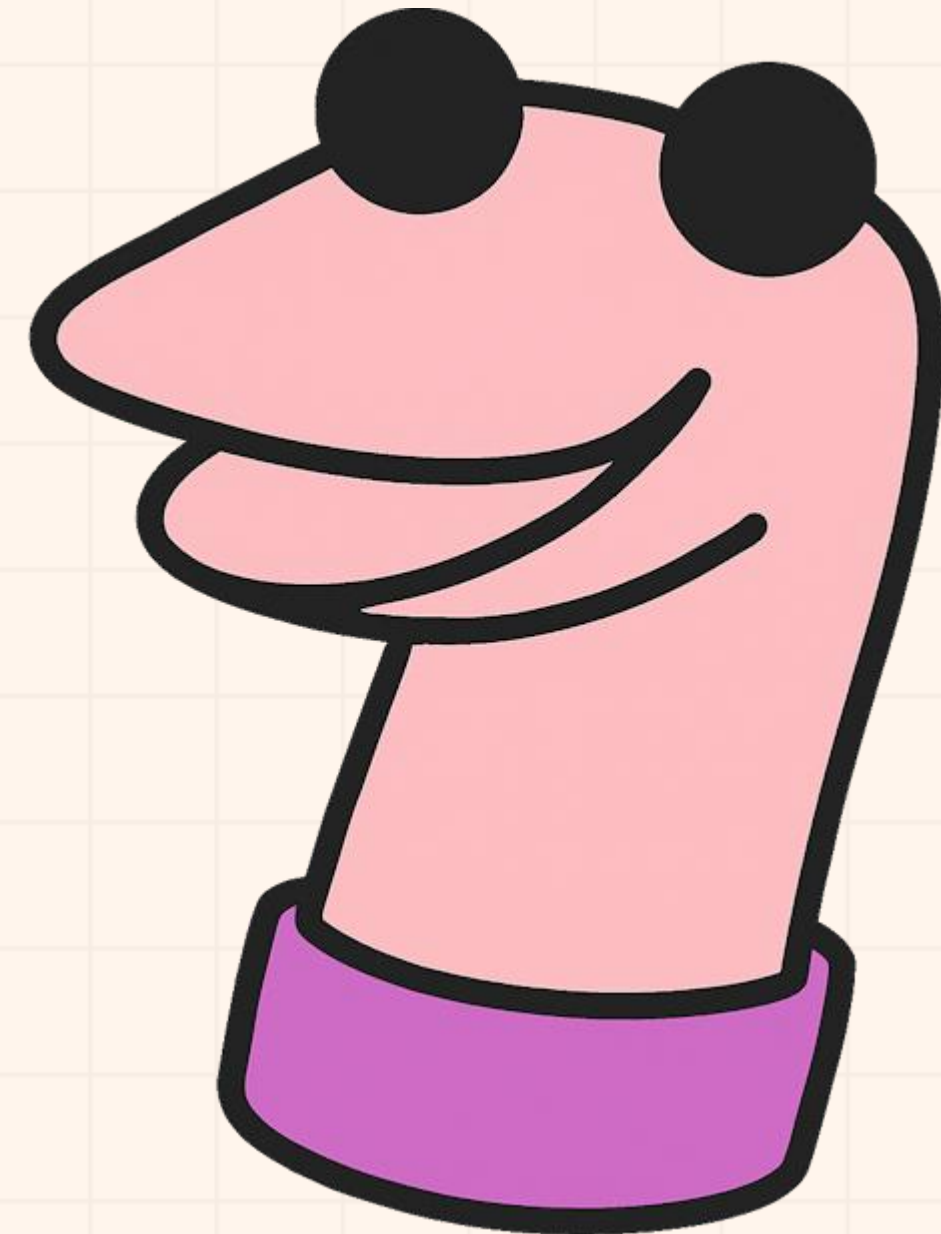
Before OSINT

Don't get under the spotlight.



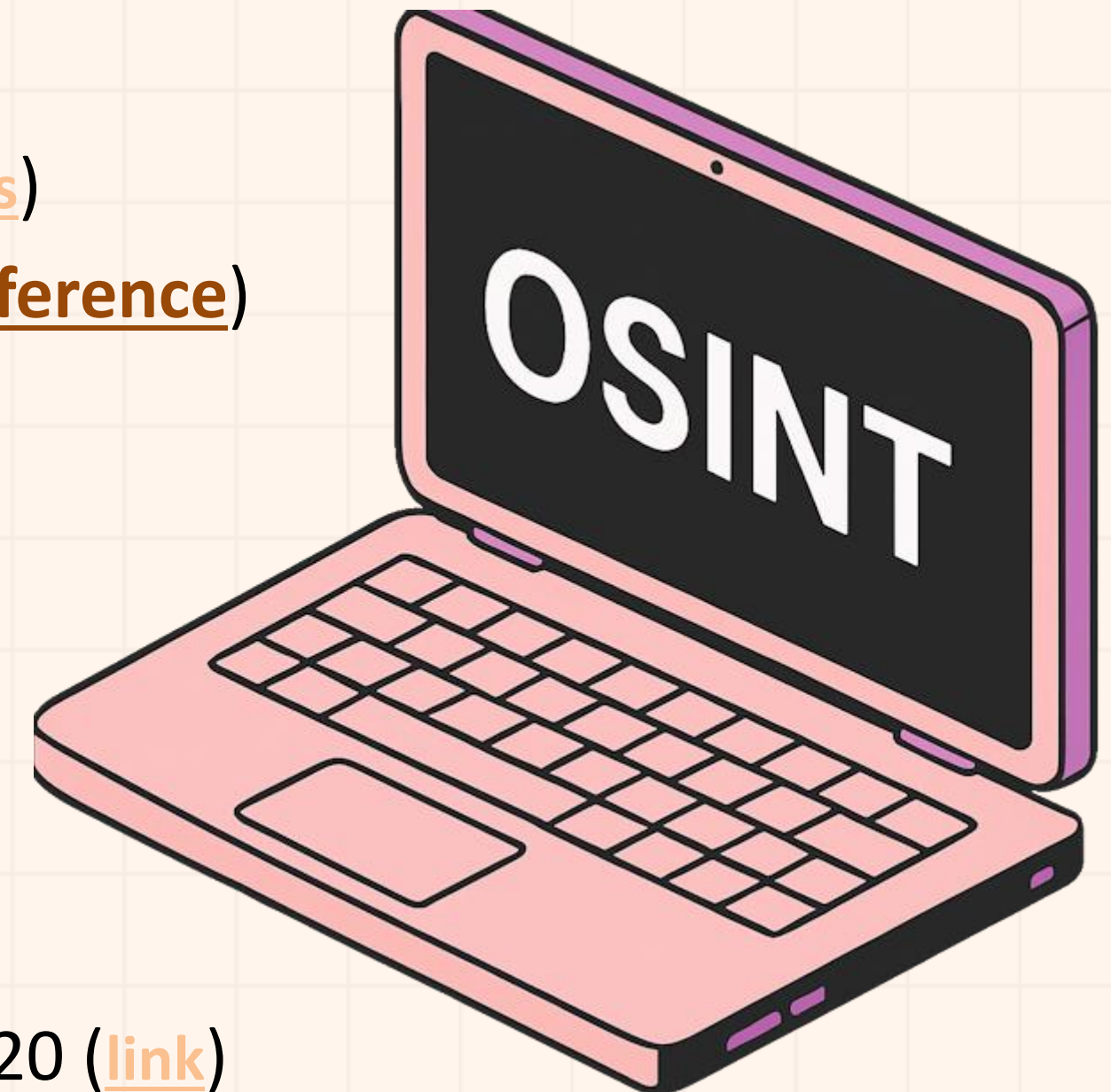
OSINT – Sock Puppet

- Temporary Email ([link](#))
- Name Generator ([link](#))
- Photo - thispersondoesnotexist ([link](#))
- Sim Card - Local / Country / Electronic
- Credit Card - Privacy.com ([link](#))
- VPN - useful to be some where else
- Email account
- Social Media accounts
- Sock Puppets Tutorials
 - The Art Of The Sock ([link](#))
 - My Process for Setting up Anonymous Sock Puppet Accounts ([link](#))



OSINT REFERENCES

- My OSINT notes ([link](#))
- Sofia Santos - Awesome tutorials and exercises ([blog](#)) ([videos](#))
- Jezer Ferreira - Must have book and conference ([book](#)) ([conference](#))
- Michael Bazzel - IntelTechniques ([link](#)) ([book](#)) ([magazine](#))
- OSINT Combine ([link](#)) ([bookmarks](#))
- OSINT Dojo ([link](#))
- OSINTCurio.us ([link](#))
- OSINT Techniques ([link](#))
- CyberDetective ([link](#))
- Open Source Intelligence Tools and Resources Handbook 2020 ([link](#))



OSINT CHALLENGES

- Sofia Santos Exercises ([link](#))
- TraceLabs CTF ([link](#)) ([notes](#))
- Hacktoria ([link](#)) ([notes](#))
- Kase Scenarios ([link](#))
- TryHackMe ([link](#))
 - My notes ([notes](#))
 - Geolocating Images Room ([link](#))
 - Google Dorking ([link](#))
 - OhSINT Room ([link](#))
 - Sakura Room ([link](#))



OSINT -Tools & more tools

- OSINT FRAMEWORK ([link](#))
- OSINT4ALL ([link](#))
- Intel Techniques ([link](#))
- OSINT Techniques ([link](#))
- Cyber Detective ([link](#))
- Aware Online ([link](#))



OSINT – Virtual Machines

- Trace Labs VM ([link](#))
- Mandiant – Threat Pursuit VM ([link](#))
- CSI Linux ([link](#))

- Tails ([link](#))
- Kali ([link](#))
- Parrot ([link](#))
- Windows ([link](#))

THANK YOU







OSINT – The Final Hours of Pop Smoke

- Rapper Pop Smoke Murdered in Home Invasion ... By 4 Masked Gunmen ([link](#))
- Instagram Posts
 - Location Tag
- Geolocation
 - Reverse Image
- Google Maps
 - Local Recon
- Airbnb/Zillow (Rent/Real-estate)
 - House photos (Outside and Inside)
 - Layout

OSINT – Other public presentations

- RootedCON - OSINT – Beware your data is out there – EDIÇÃO PORTUGAL ([link](#))
- OID2024 – OSINT – Beware your data is out there ([link](#))
- OXOPOSEC – Private Business, Public Fallout ([link](#))
- PBS - The Power of OSINT ([link](#))

<div>Portal</div> <div><div>Portal do Governo</div><div>www.portugal.gov.pt</div></div>	<div>Portal do Governo</div> <div><ul style="list-style-type: none">Membros do Governo (link)<ul style="list-style-type: none">Primeiro-Ministro (link)Redes sociais</div>
<div>Portal</div> <div><div>Ministério da Justiça</div><div>Publicações de Atos Societários</div><div>publicacoes.mj.pt</div></div>	<div>Publicações de Atos Societários</div> <div><ul style="list-style-type: none">Consultar e pesquisar todas as publicações (link)</div>
<div>Portal</div> <div><div>Portal da Assembleia da República</div><div>www.parlamento.pt</div></div>	<div>Portal da Assembleia da República</div> <div><ul style="list-style-type: none">Deputados em funções (link)Informação Pessoal (link)Registo de interesses (link)Participação em empresas (link)Dados Abertos (link)</div>
<div>Portal</div> <div><div>DRE</div><div>Diário da República Eletrónico</div><div>dre.pt</div></div>	<div>Publicações de Atos Societários</div> <div><ul style="list-style-type: none">Pesquisa (link)Site alternativo – DRE Tretas (link)</div>
<div>Portal</div> <div><div>Portal BASE</div><div>www.base.gov.pt</div></div>	<div>Portal BASE</div> <div><ul style="list-style-type: none">O Portal BASE centraliza a informação sobre os contratos públicos (link)Contratos (link)Anúncios (link)Entidades (link)<ul style="list-style-type: none">Empresas e PessoasIndicadores (link)</div>
<div><ul style="list-style-type: none">Lista de subvenções e benefícios públicos e de doações (IGF) (link)Lista pública de execuções (link)Venda de Bens Penhorados em Processos Executivos (link)Lista de devedores na Segurança Social (link)Listas de Devedores na Autoridade Tributária e Aduaneira (link)</div>	
<div><ul style="list-style-type: none">https://www.doutorfinancas.pt/empresas/como-obter-informacoes-sobre-uma-empresa/https://transparencia.gov.pt/Pesquisa de bens penhorados – não oficial (link)Pesquisa de bens penhorados – não oficial (link)https://geneall.net/https://www.einforma.pt/https://www.iberinform.pthttps://www.racius.comhttps://www.rigorbiz.pt/https://www.emailondeck.com/https://temp-mail.org/https://www.playmakerstats.com/https://www.pai.pt/</div>	