Porto Business School
University of Porto

Porto Business School

19/05/2025

Agenda

- Awareness
- OSINT
- Internet of Things
- Before OSINT

Disclaimer & Legal Considerations

Presentation is solely for educational and awareness purposes.

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

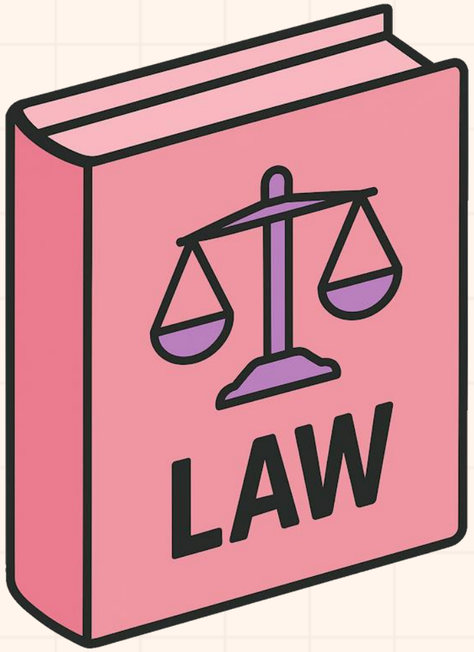
Users must check the legality of OSINT tools and methods in their country.

This presentation is <u>not related</u> to my work or employer.

images: Flaticon.com

Disclaimer & Legal Considerations

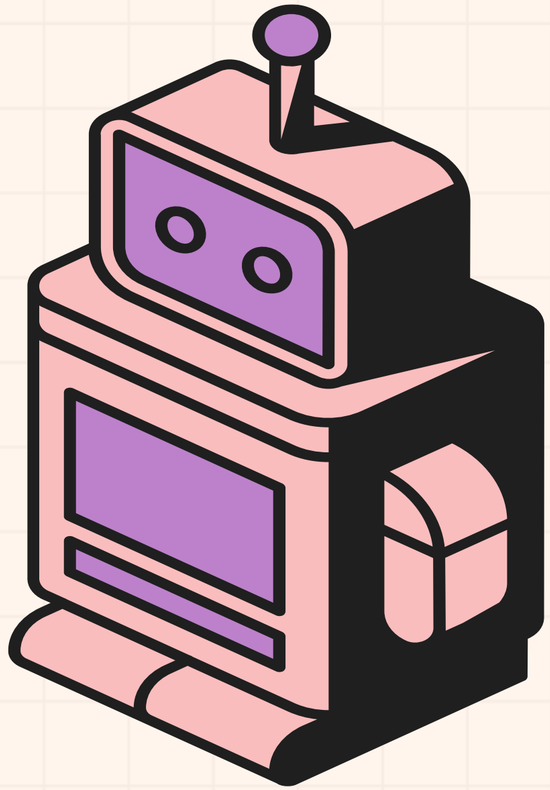
- **Portuguese Law**
  - Diário República Eletrónico (link)
  - ANACOM (link)
- **Organizations**
  - CNCS – Centro Nacional de Cibersegurança (link)
    - Incident Notification (link)
    - CERT.PT (link)
  - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) (link)
  -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

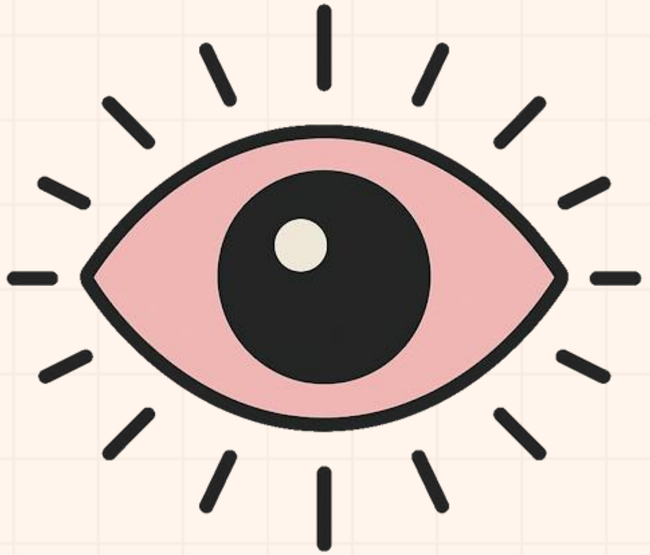
Use them all.

$whoami

👓 Pedro António Oliveira Vieira

🔐 Cybersecurity Engineer
🕵️ OSINT
✒️ Full stack developer
👨‍🏫 Public Speaker

AWARENESS

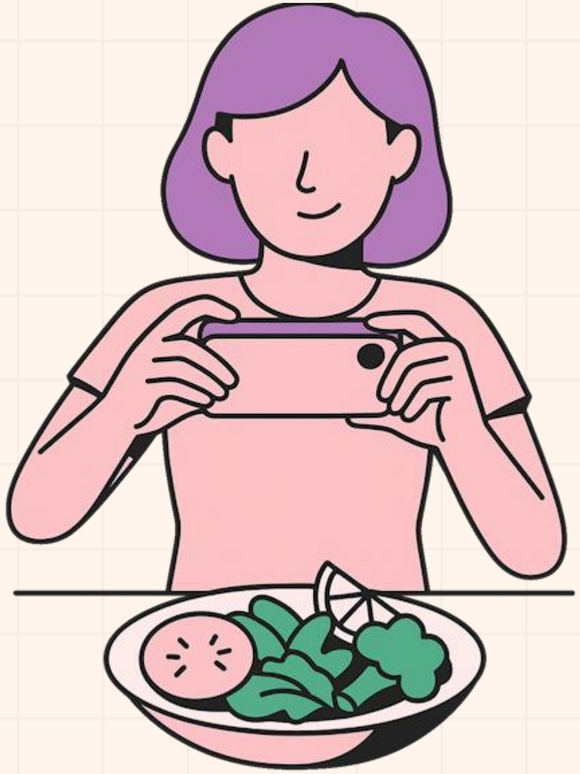


Awareness - True stories – Quiet vacations

- 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

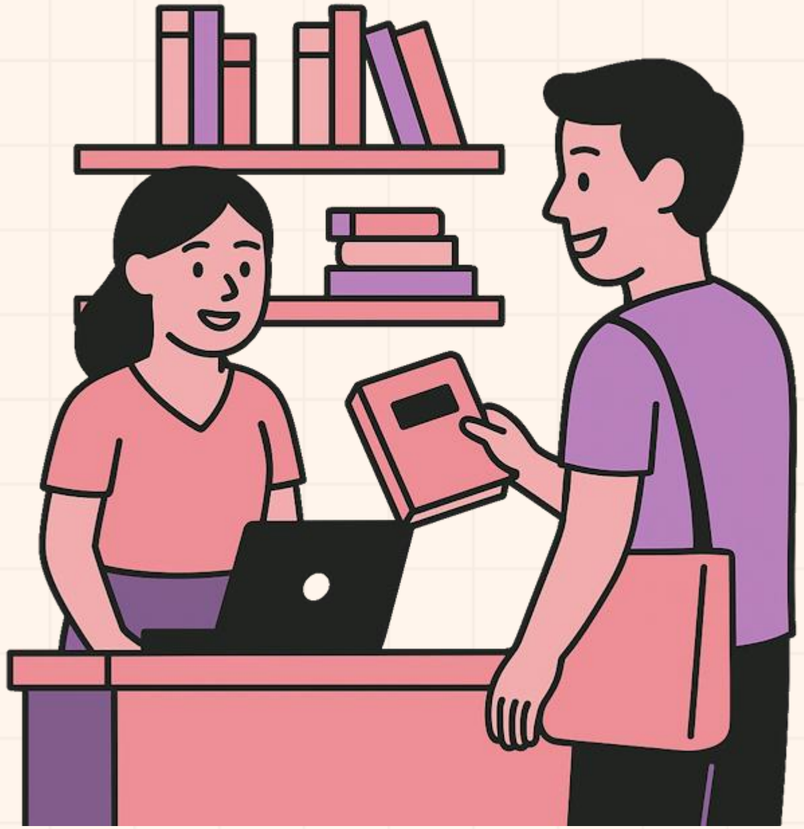


- Someone posted a photo of healthy meal during COVID
  - Working remotely on in the usual business environment
  - Company laptop was in the background
    - Zoomed in and was possible to read emails
    - Company private information could be leaked
    - **Personal information of other persons was 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)

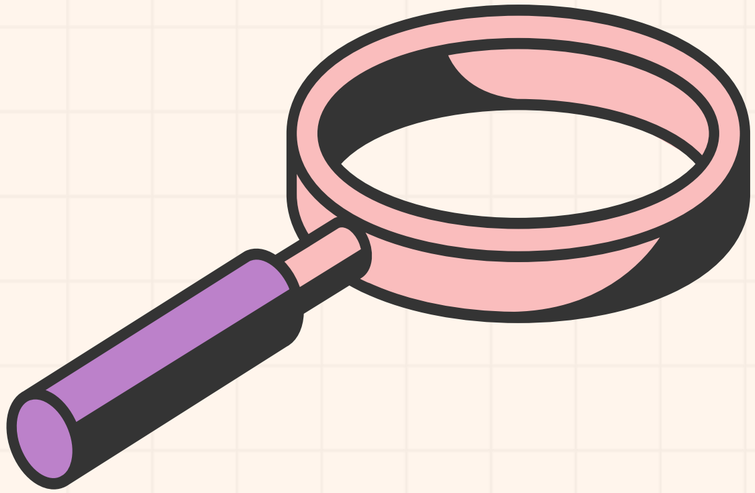
- Adding store loyalty card with phone number
  - Invoice containing:
    - Name
    - Address (Shipping address)

- 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)



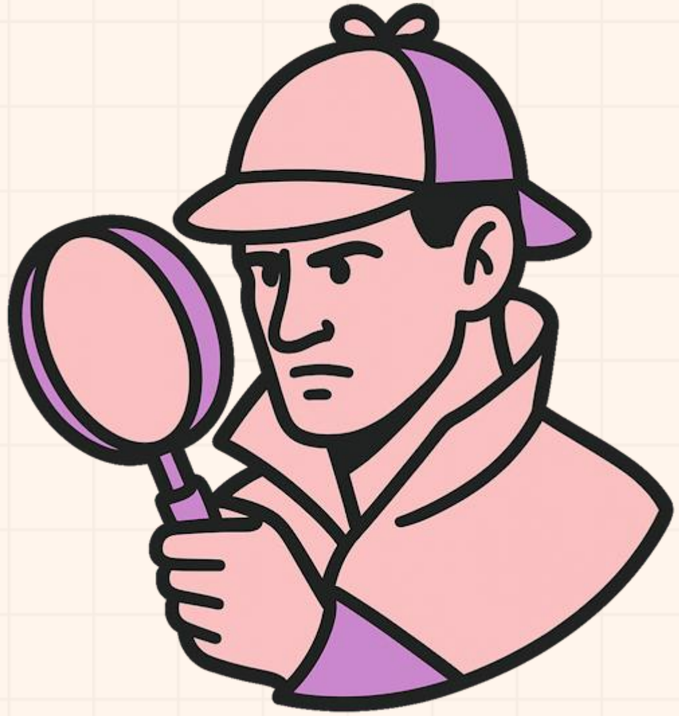
Gathering information from:

- 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

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:

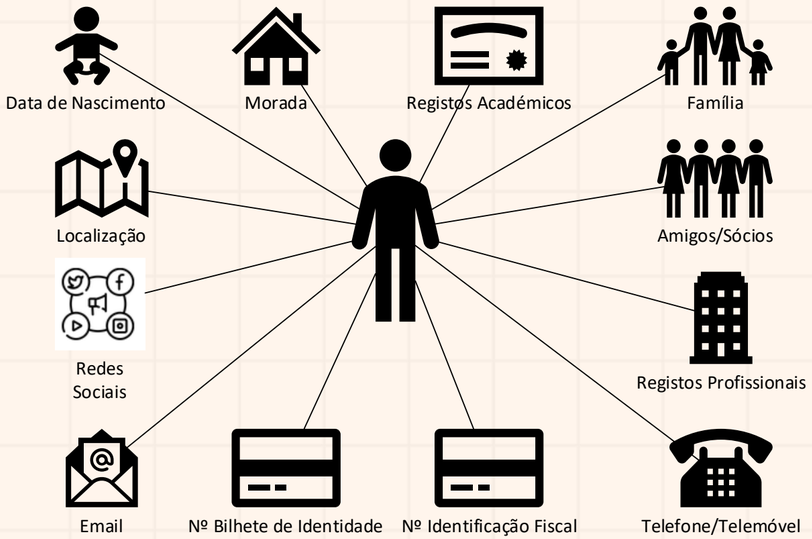
- Guides and notes on OSINT techniques
- Write-ups from platforms like TraceLabs and Hacktoria
- Training materials and curated tool lists
- Links to OSINT handbooks and educational videos

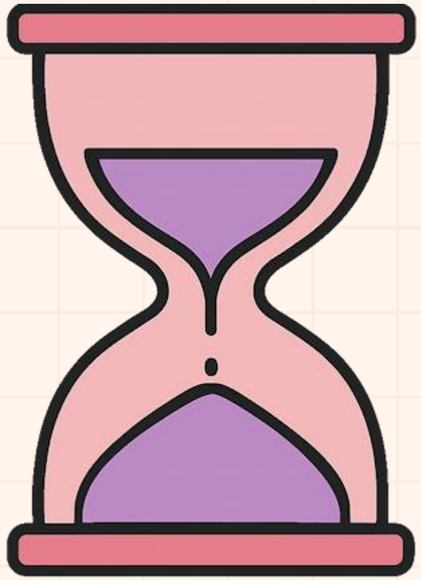
💼 Professional Role

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

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.

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)

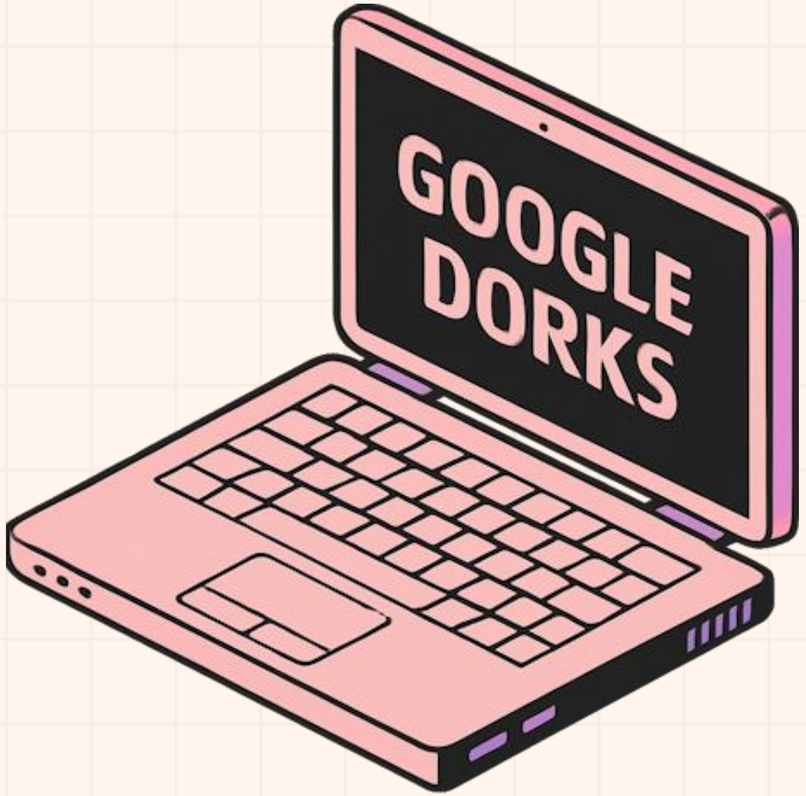
Improve the search - Search operators

- **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)



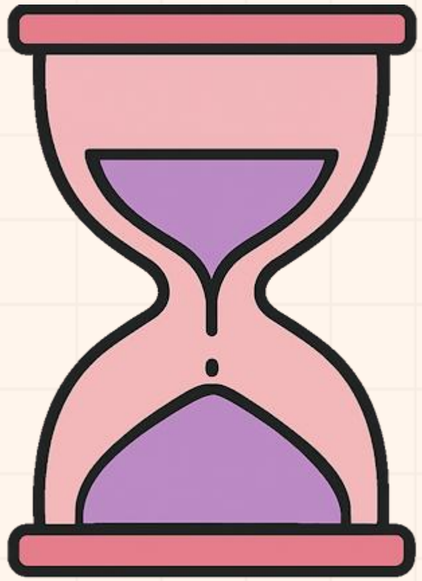
Improve the search or “Go lazy” – Go IA

- 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

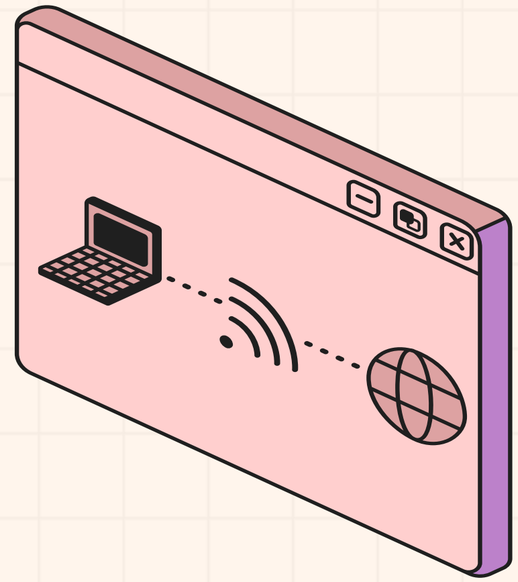
Well, at least some commercial models



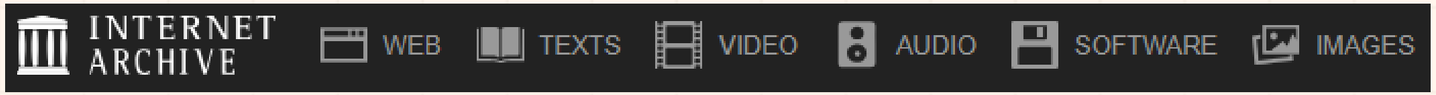
EXERCISE TIME

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)



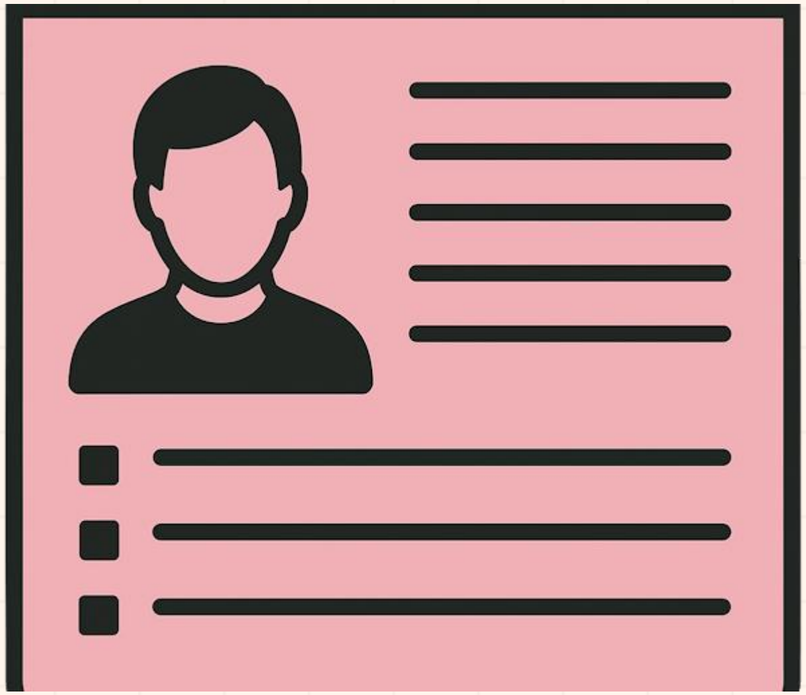
- The internet has memory
  - Arquivo.pt (link)
    - Example (**link**)
  - Internet Archive - Wayback Machine (link)



    - 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.

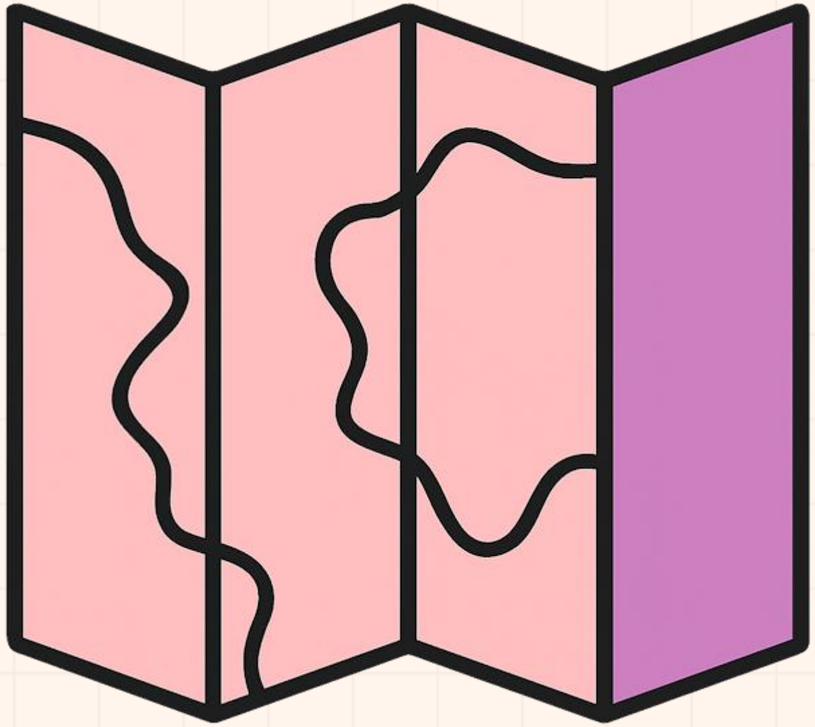
OSINT - Maps

- 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

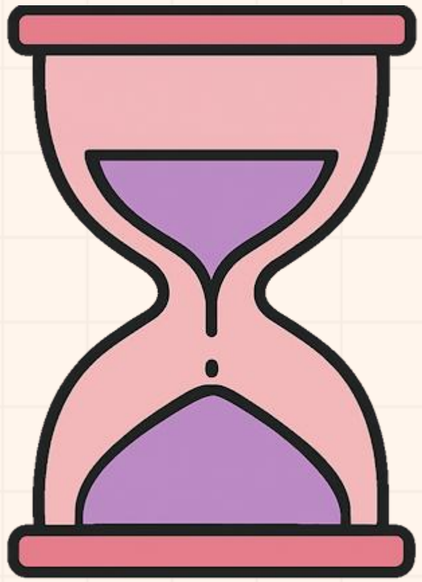
- One image is worth 1000 words, maybe more.
  - What information can be extracted from a photo ?

- 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)



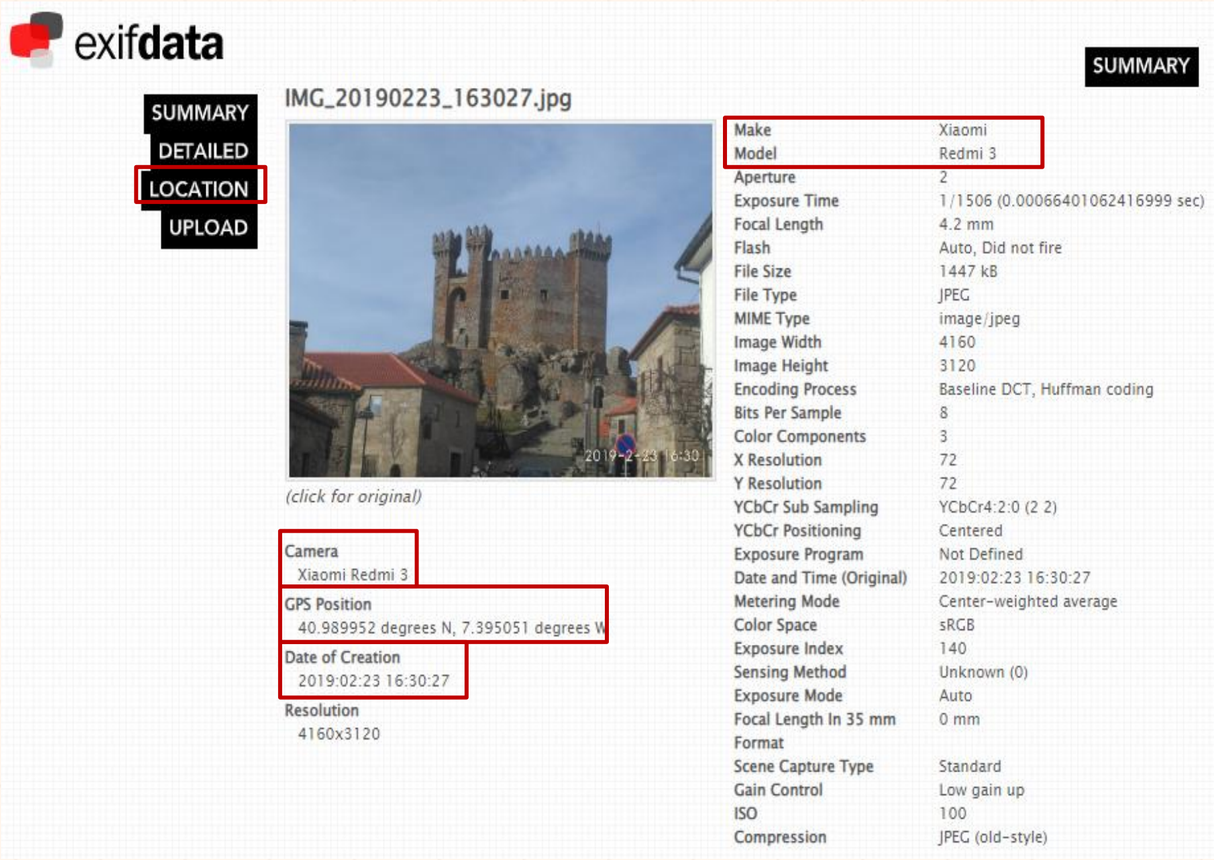
EXERCISE TIME

OSINT – Photos - Identify the location

- An image is worth a thousand words

- File analysis
  - Metadata
  - GPS (link)
  - Google Maps (link)

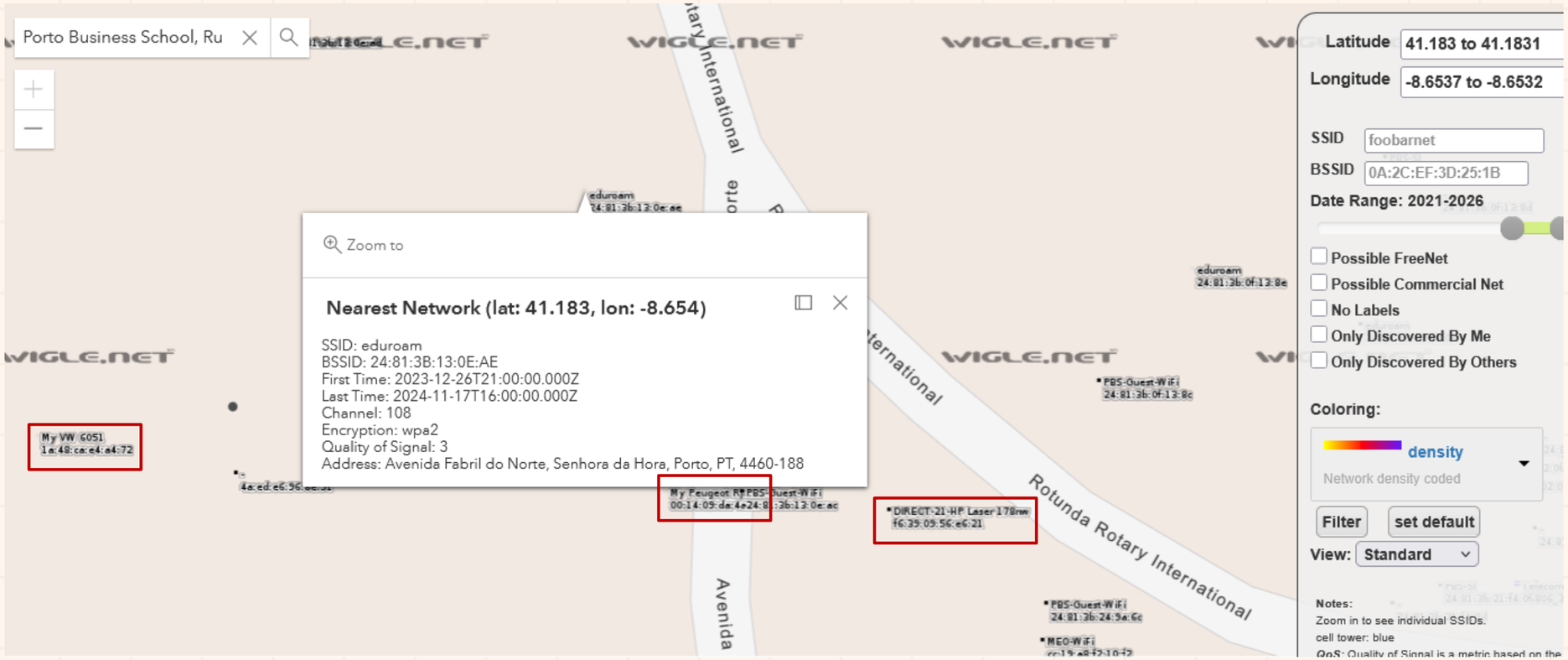
- Tools
  - CleanUp (link)
  - AperiSolve (link)



OSINT - World Map - WiFi Networks

- Wiggle (link)

- Routers
- Printers
- Cars
- IoT
- …



OSINT - World Map - WiFi Networks

- Wiggle (link)

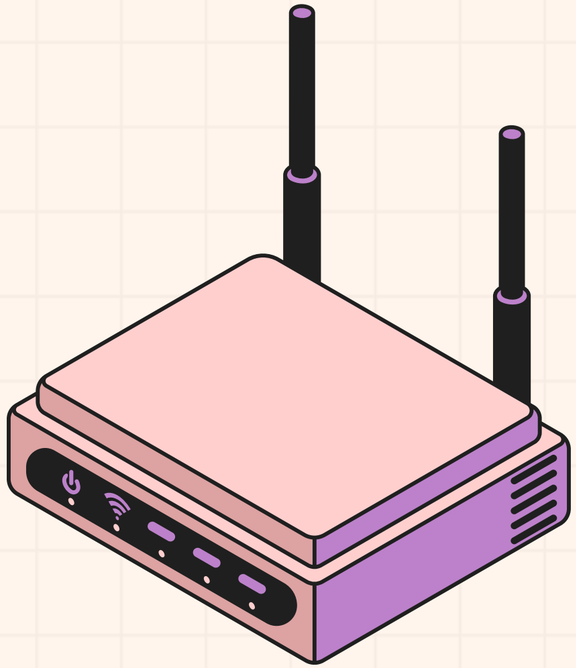
Zoom to

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
SICAE Sistema Informação da Classificação Portuguesa de Atividades Económicas SICAE www.sicae.pt	• 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
REPÚBLICA PORTUGUESA JUSTIÇA Ministério da Justiça Publicações de Atos Societários publicacoes.mj.pt	

Data	Entidade	Concelho	Acto/Facto			
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

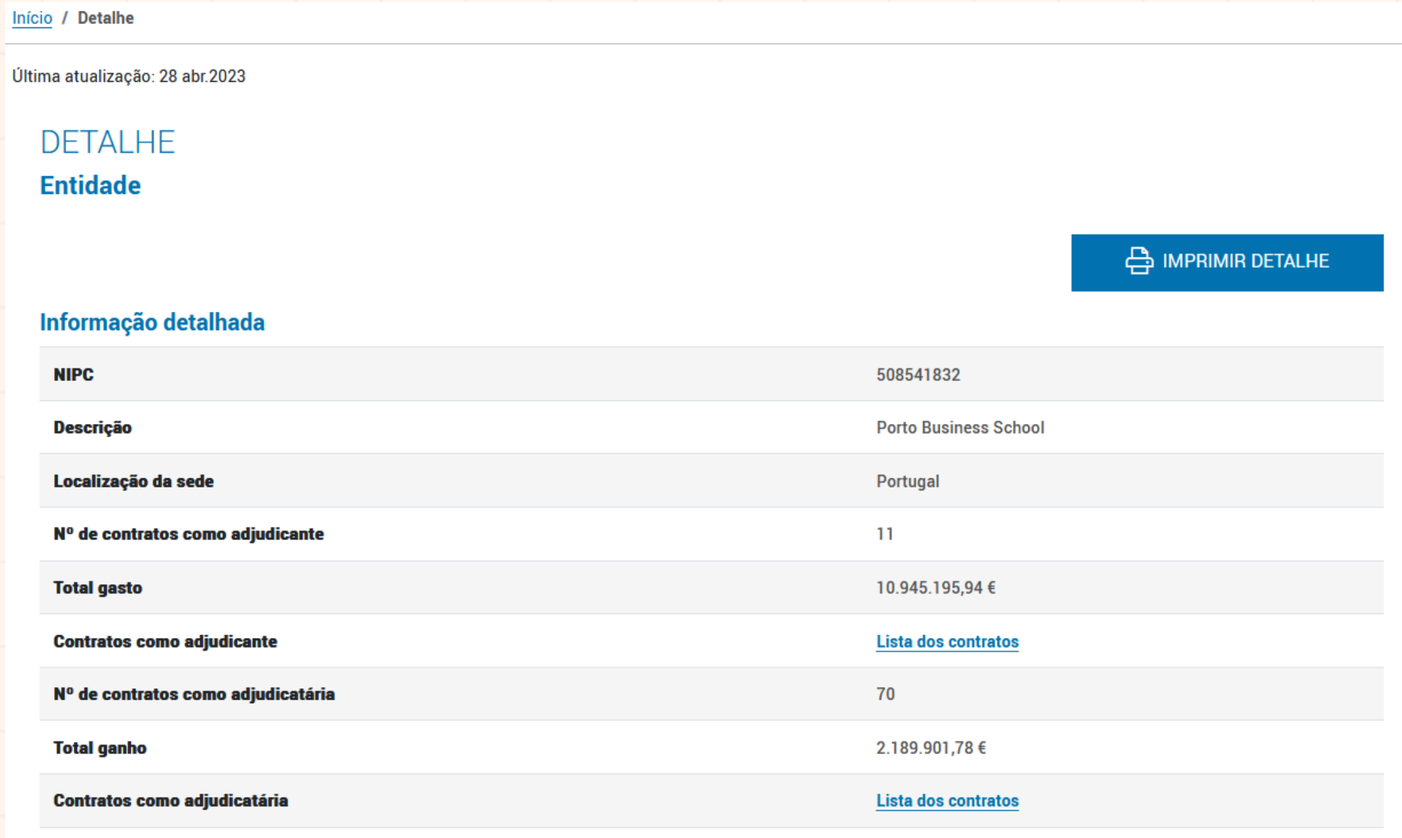
Demo Time

IMPIC base: CONTRATOS PÚBLICOS ONLINE

Portal BASE

www.base.gov.pt

- Entity (**link**)
- Contracts (**link**)



Início / Detalhe

Última atualização: 28 abr.2023

DETALHE

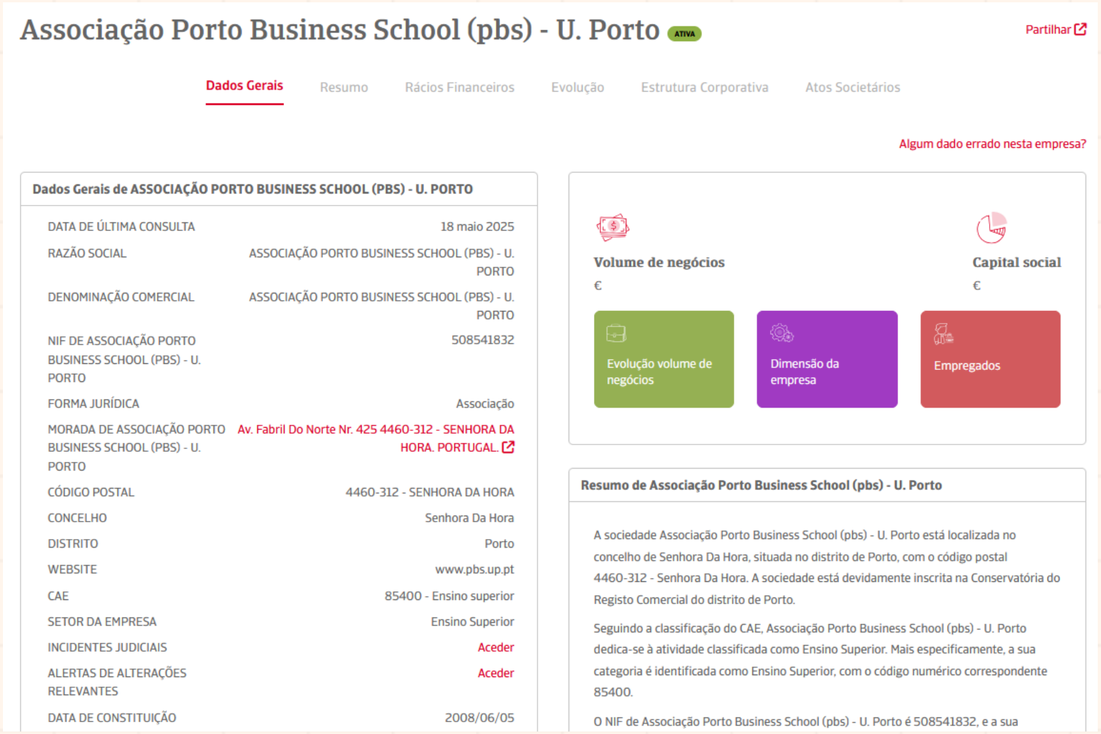
Entidade

IMPRIMIR DETALHE

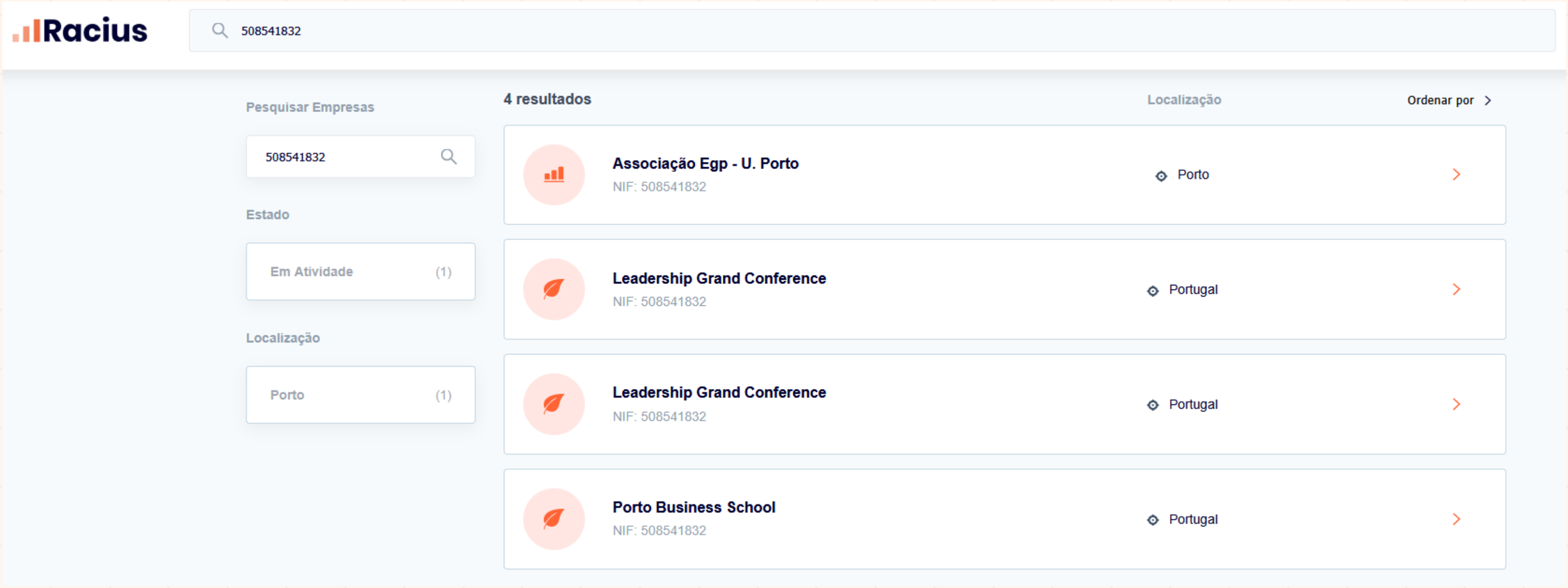
Informação detalhada

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

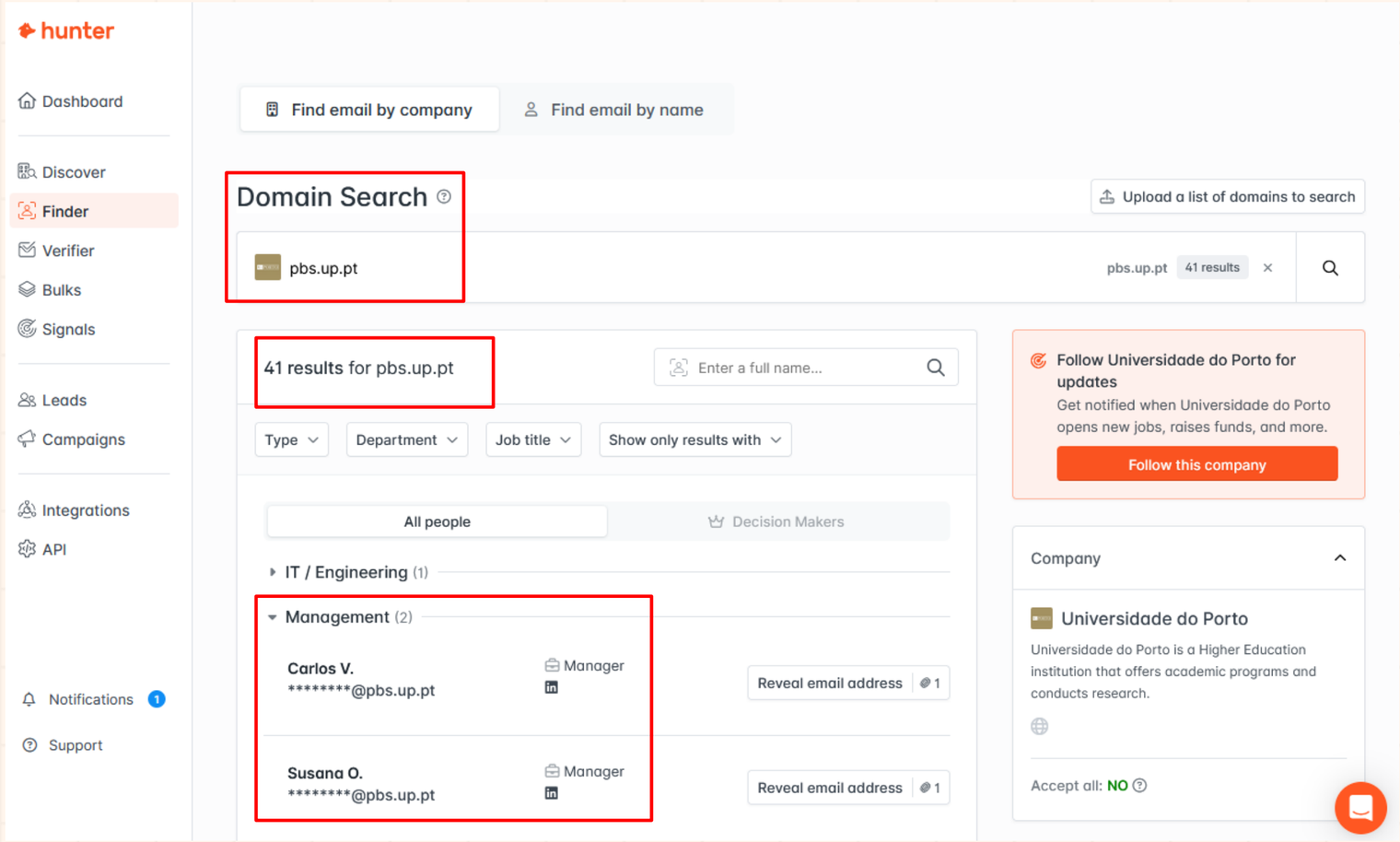
OSINT - Companies



OSINT - Companies



OSINT - Companies



OSINT - Vehicles

Portal	Automóvel On-line

automóvel online
Automóvel On-line
www.automovelonline.mj.pt
	• Certidão Permanente do Registo Automóvel (link)
	  • Document example (link)
	• **Demo**: search for a car (link)
	  • License Plate : 89-QS-04 (link)

Portal	IMT - Instituto da Mobilidade e dos Transportes

IMTonline.pt O Futuro da Mobilidade
Instituto da Mobilidade e dos Transportes
www.imtonline.pt
	• Serviços IMT online.pt (link)
	  • Veículos → Certidão
	  • Mandatory inspection
	  • Vehicle characteristics

Portal	ASF – Autoridade de Supervisão de Seguros e Fundos de Pensões
ASF AUTORIDADE DE SUPERVISÃO DE SEGUROS E FUNDOS DE PENSÕES ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões www.consumidor.asf.com.pt	• Check Insurance (link) • License Plate : 89-QS-04

Portal	Lastvin
LastVIN.com Mercedes-Benz VIN Decoder LastVIN.com www.lastvin.com	• Mercedes-Benz VIN Decoder (link) • Will the prime-minister keep the car?

Hack across the globe by VIN (link)

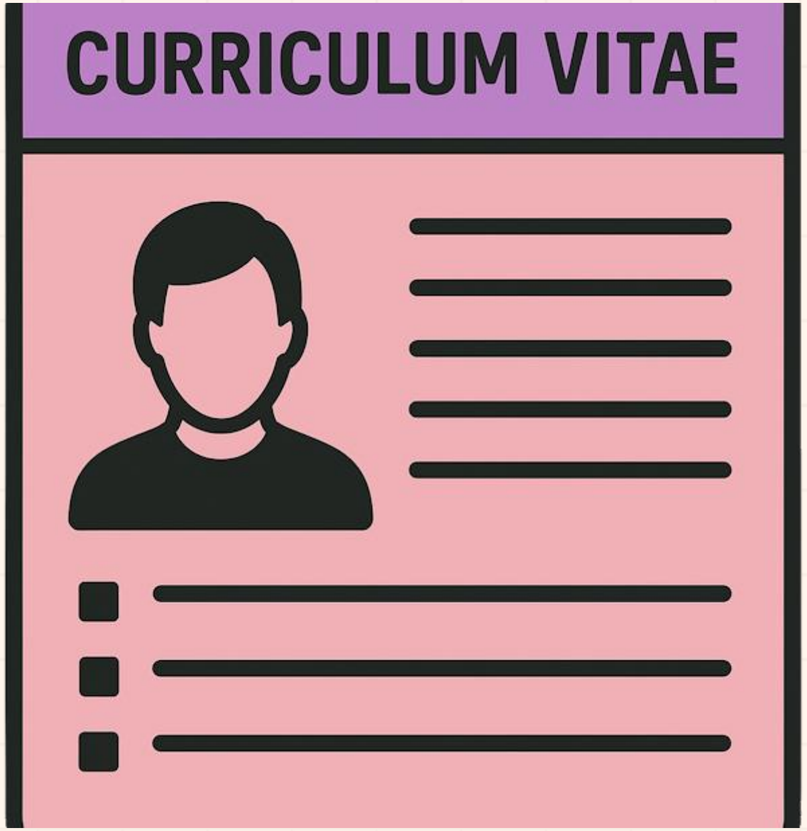
AITI – Brunei Darussalam

AITI Authority for Info-communications Technology Industry of Brunei Darussalam

BEWARE
YOUR DATA
IS OUT THERE

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 vencimento” filetype:pdf
  - “recibo de vencimento” – 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)

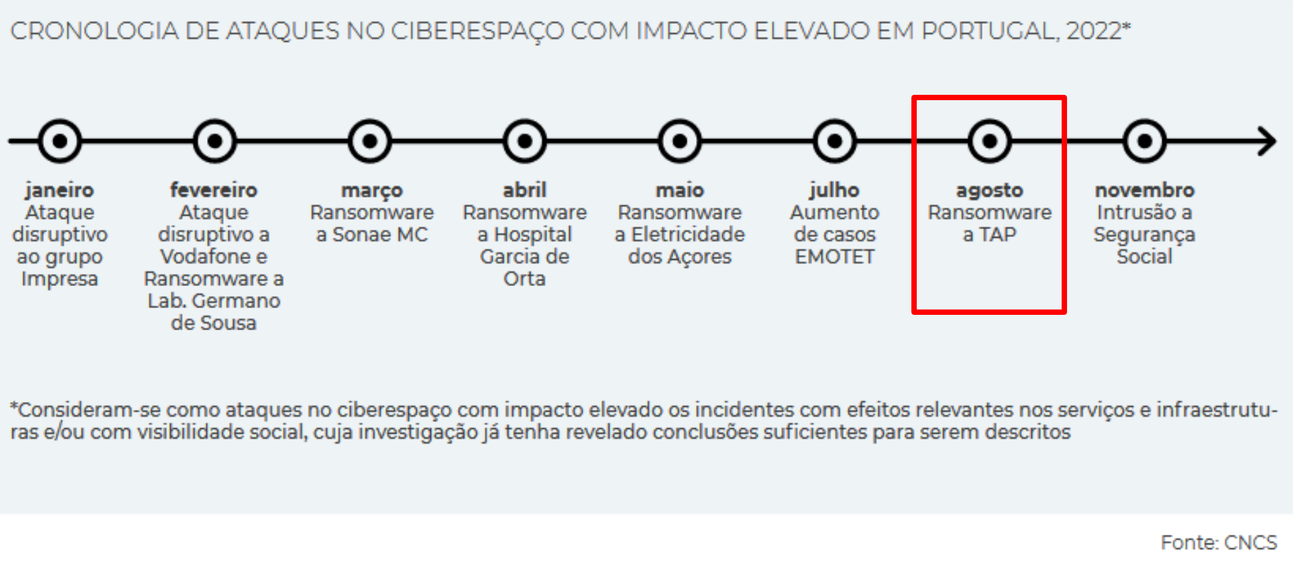
- About 6.200 results
  - Sites / pages that were “tagged”/”signed”
  - Attack and contents changed to show off skills (mainly kids)
    - compared to street tagging

Data breach - When companies are hacked

- When companies are hacked, private data is exposed. Private data becomes “public”. (**link**)

- Troy Hunt
  - HaveIBeenPwned (**link**)
  - Pwned websites (**link**)
  - Domain search (link)

- CNCS Report
  - Cybersecurity in Portugal 2024 (link)
  - Cybersecurity in Portugal 2023 (link)



Data breach - Credentials

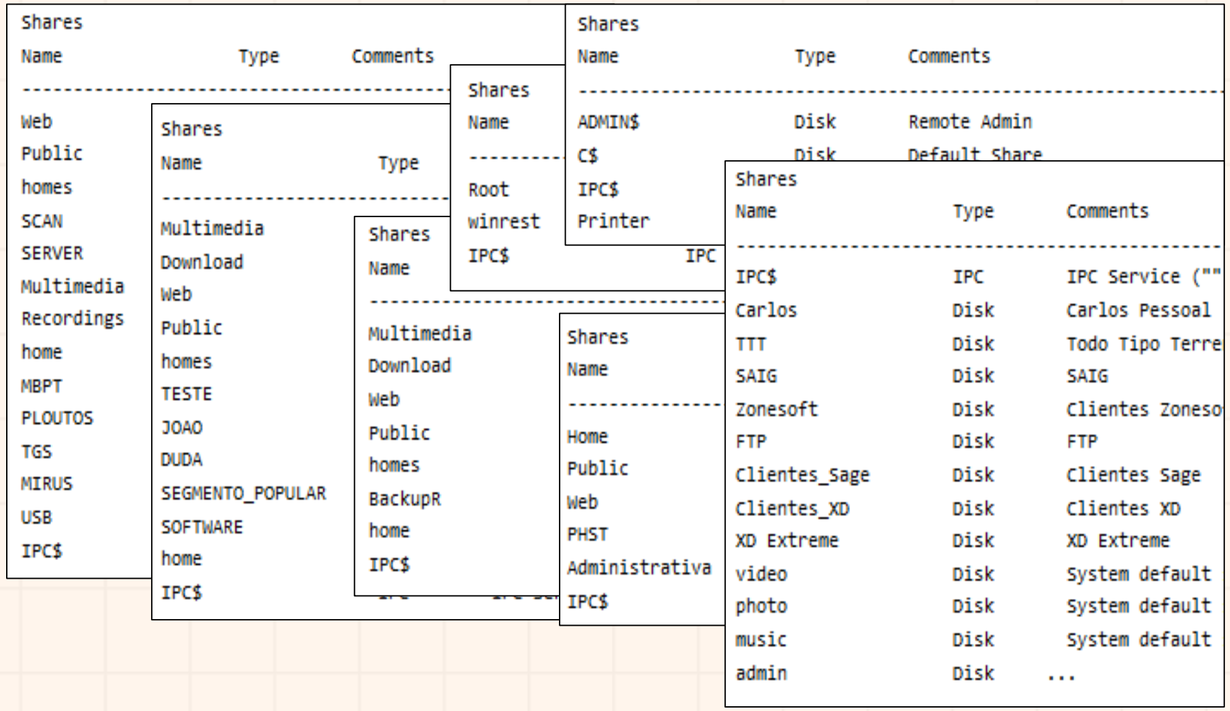
- Source
  - “Publicly” available list of credentials
- Information gathered
  - Rule of email/login
  - Rule of password complexity
  - List of users
    - Phishing campaigns
    - Brute force
- Look for those users on Social Media
  - Reuse of credentials

Data 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

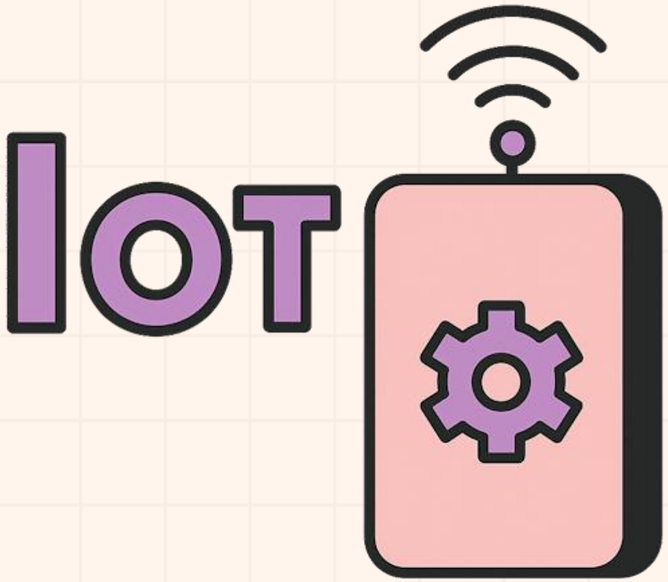
- Shared folders accessible to 8 thousand million people (link)
  - Contabilidade – 6
  - Clientes – 3
  - Faturacao – 1
  - Primavera – 6
  - SAGE – 13
  - Winrest – 148



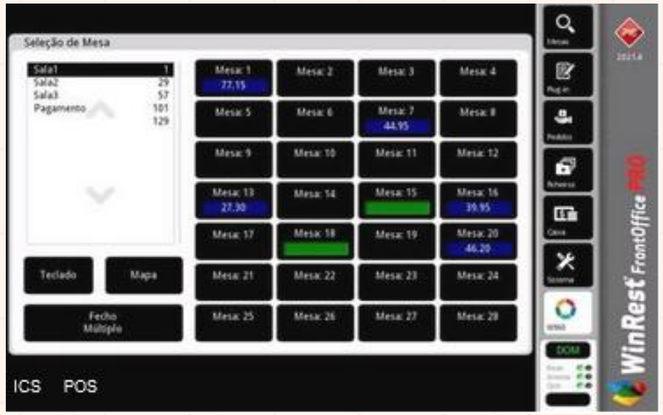
Message from Ella

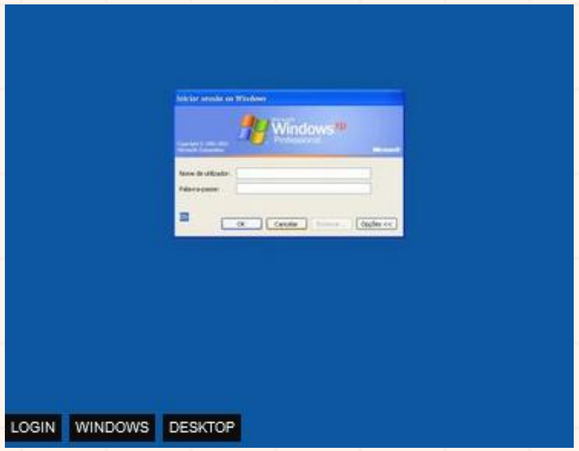
Deutsche Telekom
Message from Ella | Without Consent

Internet of Things

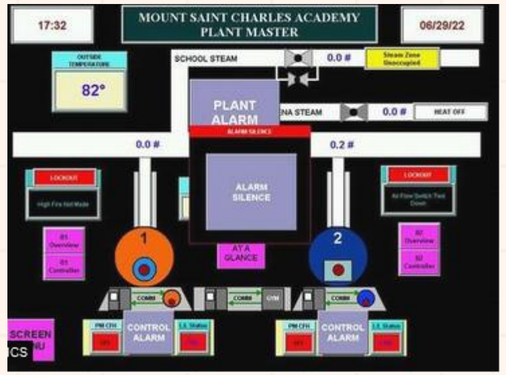


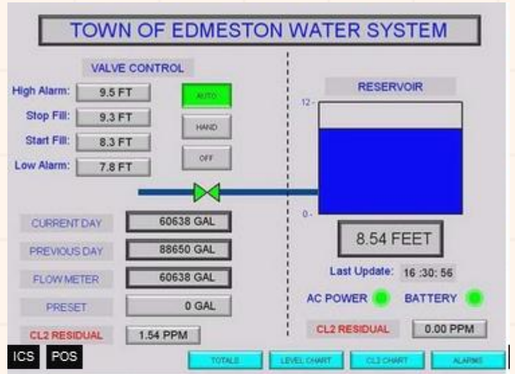
OSINT - Shodan – IoT Search Engine

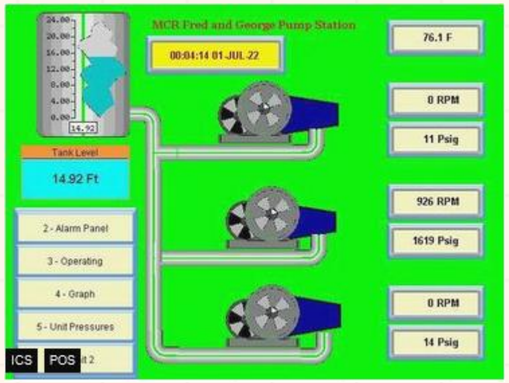




OSINT - Shodan – IoT Search Engine







OSINT - Shodan – IoT Search Engine

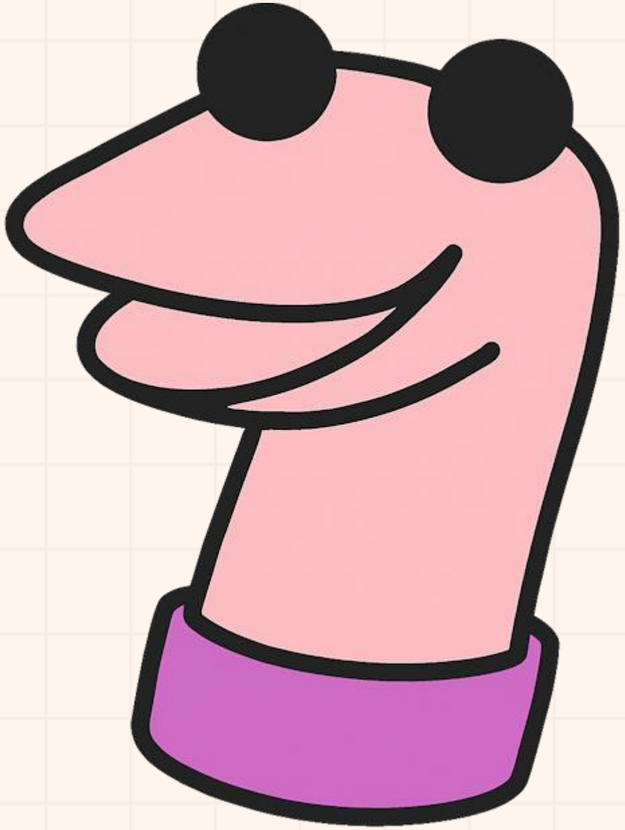
- Internet Exposure Observatory
  - Exposure Dashboard (**link**)
- Explore
  - Shodan explore (**link**)
- Images
  - Shodan images (**link**)
- Maps
  - Shodan maps (link)
- Remote Desktop (**link**)
  - Total results: 2,745,593
  - Braga (link)
- Imagens
  - Braga (link)
  - VNC Remote Access and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

Before OSINT

Don’t get under the spotlight.

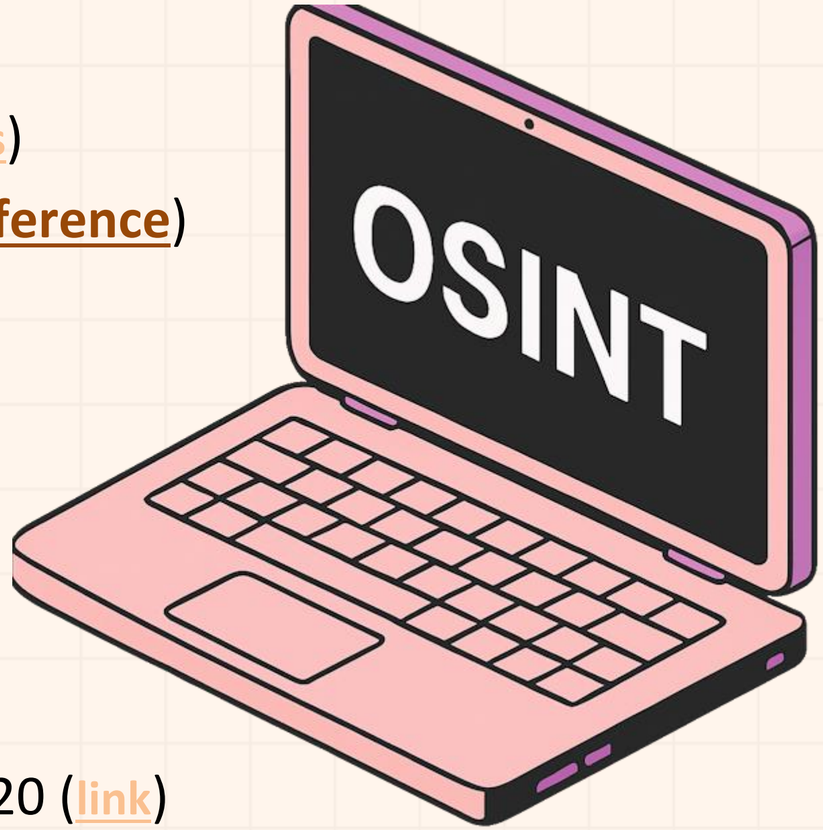
OSINT – Sock Puppet

- 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)
- 0XOPOSEC – Private Business, Public Fallout (link)
- PBS - The Power of OSINT (link)

Portal	Portal do Governo
	• Membros do Governo (link) • Primeiro-Ministro (link) • Redes sociais

Portal	Portal da Assembleia da República
	• Deputados em funções (link) • Informação Pessoal (link) • Registo de interesses (link) • Participação em empresas (link) • Dados Abertos (link)

Portal	Portal BASE
	• O Portal BASE centraliza a informação sobre os contratos públicos (link) • Contratos (link) • Anúncios (link) • Entidades (link) • Empresas e Pessoas • Indicadores (link)

Portal	Publicações de Atos Societários
	• Consultar e pesquisar todas as publicações (link)

Portal	
	• Pesquisa (link) • Site alternativo – DRE Tretas (link)

• 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)

• 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.pt • https://www.racius.com • https://www.rigorbiz.pt/ • https://www.emailondeck.com/ • https://temp-mail.org/ • https://www.playmakerstats.com/ • https://www.pai.pt/