OSINT

Beware. Your data is out there.

OSINT – Open-source intelligence Digital Footprint

- 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)

- It's about digital footprint. Gathering information from:
  - search engines (Google, …)
  - social media (Facebook, …)
  - government sites
  - …

- The constant battles:
  - Privacy vs Publicaly available information
  - Convinience vs Security

Disclaimer & Laws

Disclaimer
Boring but necessary

- Information in this presentation is intended for **educational and awareness purposes only**.
- **Live presentation**. Not a controlled environment and some contents may be inappropriate for some users.
- **I accept no responsibility** in any kind for the use, misuse, downloading, viewing in whatever way the links in this presentation.
- This presentation is not related to my work or employer.

Disclaimer
Avoid illegal activities

- Some links, websites, software or other items listed may or **may not be legal**, illegal, a felony, misdemeanor, or worse, in your country.
- Please make sure that you are **allowed** to browse the websites, download links and software **BEFORE USING**!
- Ignorance about laws or rules is **no excuse** for illegal activities or wrongdoing.
- Illegal activities may get you in **trouble or arrested**.
- **Always check what is legal, and what laws apply**.

Laws
Portuguese Law and Organizations

- Laws
  - 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)

Search, and then search again

Who Am I
Let's OSINT me ☺

- Just got a name
  - Pedro António Oliveira Vieira
- Google (link) ➡
- Google "Improved Search" (link) ➡
- Google "Improved Search" (link) ➡
- LinkedIn (link) ➡
  - Public profile was showing way too much

- Certified **Ethical** Hacker (link) ➡

Who are YOU
Search yourself

- Search your name on Google and analyze the results
  - As you saw the search can be improved
- Some results can/will include:
  - Family and Friends
  - Work
  - School grades
  - BI - Identity Card Number (yes)
  - NIF – Tax Identification Number
- 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)
- Yahoo (link)
- DuckDuckGo (link)
- Baidu (China) (link)
- Yandex (Russia) (link)

- You may ask to be removed from one search engine, not all ☹

Google Dorks
Commonly used searches

- Google Advanced Search (link) ⇨
- Google Hacking Database (link)
- gbhackers (link)
- google-dork-list (link)
- Google Advanced Operators Guide (link)
- Google Advanced Operators Reference (link)

Search operators
Improve the search

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

- **42 Advanced Operators** (link)

Search
Dork Examples – 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, …

Search
Dork Examples - Hacked

- Google Search (link) ➡

- allintitle:“hacked by” site:pt
  - “hacked by” - keyword to look for
  - site:pt - only “portuguese” sites (registered portuguese domains)

- About 13.400 results
  - Sites / pages that were “tagged”/”signed”
  - Attack and contents changed to show off skills (mainly kids) – compared to street tagging

Awareness

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 on other persons was showing
  - Social Media Apps use OCR
    - Means they also read the emails
    - And everyone else on that social media could get the same information

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 – 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 and full name were not mine ☺

Awareness
Life is hard

- What companies know about us (link) ➡
- Awareness
  - What do we teach our kids? Do we teach ?
  - They are exposed to everyone on the internet.
- Social Media accounts
  - If you don't have Facebook, I can create one in your name and call your friends

Awareness
Browser F12

- 1 - Type url on browser
- 2 - Page is requested from the internet
- 3 - Page is displayed from local data (previously downloaded)

- Show password text on password field
- Did you ask for a screenshot
  - Let me just change some data

OSINTing

OSINT
Personal Information

- Posted information can get publicly and world available
  - Even private profiles can have their data shared by others
- When information is posted
  - Shows where you are at that time (habits & routines)
- Information on the picture
  - Metadata
  - Geolocation

Deadly Social Media
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

- YouTube Video: The Cyber Mentor (link)

OSINT
Tools & more tools

- OSINT FRAMEWORK (link) ➡
  - Yups, only one link is enough

OSINT Profiling

- What's my IP? (link)
- Ip2Location (link)
- Mylocation (link) ➡
- Twitter
  - Twitter Advanced Search (link) ➡
- Facebook
  - StalkFace (link) ➡
  - Sowdust Github (link)
  - IntelligenceX Facebook Search (link)

OSINT
Profiling

- Mobile (how long have you been using the same number)
  - Sync me (link)
- Usernames (you reuse usernames)
  - NameChk (link)
  - WhatsMyName (link)
  - NameCheckup (link)
- Tinder
  - Username reuse (link)
- New awesome tools are always being created

OSINT
Profiling - Professional

- LinkedIn (link) ➡
- Xing (link) ➡

- Curriculum Vitae
  - Sending CV with too much information – what is too much ☺
    - Home address – Street View

- Company Information
  - Technologies described in job adds (leaking information)

- Professional information phishing
  - Fake job adds (Is this a thing?)

OSINT PT

OSINT
Portugal – Public contracts

- Base (link)
  - The example (link)
- PDF of contract with PII strikethrough (link)
  - Open with pdf reader and delete the strikethrough boxes
  - Name of employee who edited the document
    - Information on UA, LinkedIn, Facebook, …
  - Metadata: “KONICA MINOLTA bizhub C454”
- Information leaked
  - Full Names, nif, addresses

OSINT
Portugal – Vehicle Information

- Automóvel On-line (link)
- Certidão Permanente Automóvel (link)
  - License Plate : “01-EF-34”
  - Result
    - Brand: MERCEDES-BENZ
    - VIN: WDD2040081A043326
  - Example (link)
- Vehicle Information (link)
  - Example (link)
  - Information: Brand, Model, Location, Paint, Delivery Date, Extras, …
- Hack across the globe by VIN (link)

OSINT
Portugal –Insurance Information

- ASF – Autoridade de Supervisão de Seguros e Fundos de Pensões (link)
  - Example (link)
    - License Plate : “01-EF-34”
    - Date : “03-07-2022”
  - Example 2 (link)
    - License Plate : “01-EF-34”
    - Date : “03-07-2012”
- Insurance Company
  - Current and Past
  - Length of the contract
  - Insurance policy number
  - Is it possible to get information for all license plates ????

OSINT
Portugal Specific

- Registo Predial Online (link)
- DGES - Direção-Geral de Ensino Superior (link)
- DRE - Diário da República (link)
  - Search DRE (link)
- Finanças - Penhorados (link)
  - Example (link)
  - Search Penhorados – (link)
- Ministério da Justiça - Penhorados (link)
- Plataforma Eletrónica de Compras (Administração Pública) (link)

- Leaked information:
  - Full Names, Addresses, NIF, Company, Marital Status, …

Free to Share

License

- Feel free to use/modify/share
- Teach someone
- Improve awareness