REMOTE HIRING or REMOTE SCAMMING? A PRACTICAL OSINT INVESTIGATION & DUE DILIGENCE

Table Of Contents

- Open-Source Intelligence (OSINT)
- Due Diligence in OSINT
- Objective of This Project
- Companies Used in the Case Study
- OSINT Tools For Deep Technical Conversation
    - theHarvester
    - Spiderfoot
    - Photon
    - Holehe
    - Recon-ng
    - HaveIBeenPawned
- Social Media + People Search Tools
    - LinkedIn
    - Freepeoplesearchtool
    - Whatsmyname
    - Google Dorking
    - Core Google Dorking Operators With Simple Examples
    - Boolean Logic & Filters In Google Dorking
- Domain & Company Identity Verification

In today’s globally connected world, remote job opportunities have become more accessible than it was, before. Online platforms like LinkedIn, Indeed, Upwork, Glassdoor, Fiver, Telegram or WhatsApp groups constantly advertise lucrative remote roles, often with attractive pay and flexible work schedules. However, this digital openness has also given Cybercriminals the perfect cover to exploit unsuspecting job seekers by posing as recruiters/HR personnel from fake companies, or impersonating a staff of a real company for dubious reasons.

This project aims to showcase how **OSINT** and **Due Diligence** can be used to verify the authenticity of remote job offers, especially when a candidate receives an offer from an unfamiliar company. Whether you're a job seeker, a cybersecurity student, or simply a curious digital citizen, the techniques demonstrated here can help you separate real opportunities from scams.

Open-Source Intelligence (OSINT)

Osint is known to be the process of collecting, analyzing, and using information from publicly available sources to produce actionable & resourceful intelligence. The sources used in gathering the intelligence could be websites, social media platforms, articles, government records, personal publications, domain registries, metadata from files or images and many more sources. Having **OSINT** skills is important & key for those in fields like; Cybersecurity, Law Enforcement, National Security, Military, Journalism, Human Resource etc. Beyond the above-mentioned fields, knowing how to use **OSINT** tools is also an added advantage for various purposes, Threat Hunting, Reconnaissance, Fraud Detection, and in this context, company/recruiter verification.

The major strength of **OSINT** rests on the basics that it is **LEGAL & EASILY ACCESSIBLE**. It involves data that's already available, which directly means no hacking or unauthorized access is required. However, the challenge lies in which particular tools to use, filtering through large volumes of data, validating its authenticity, and ensuring its relevance to the investigation or research at hand.

Due Diligence in OSINT

Due diligence in the context of OSINT refers to the thorough and methodical process of gathering and validating information to assess the reliability, legality, and completeness of the data. This is crucial when;

- Investigating individuals or entities (e.g., in background checks, financial investigations, or fraud detection),
- Evaluating potential business partners or acquisitions,
- Ensuring compliance with legal and regulatory requirements,
- Conducting risk assessments in Cybersecurity.

Due diligence ensures that any decisions or actions taken based on OSINT findings are based on verified, relevant, and contextualized data. It involves cross-referencing multiple sources, checking timestamps, verifying ownership of digital content, and identifying potential biases or misinformation.

[Back to top]

OBJECTIVE OF THIS PROJECT

To assess the authenticity of a remote job offer by conducting thorough background checks and due diligence on the prospective employer or organization. This investigation will leverage practical Open-Source Intelligence (OSINT) tools and techniques to gather verifiable information, identify red flags, and evaluate the digital footprint of the entity. The findings will be documented in detail, with a comparative analysis drawn between a suspicious (potentially fraudulent) company and a legitimate, verified organization to highlight key indicators of authenticity versus deception.

Companies Used in the Case Study

(I) Suspicious/Fake Company (for OSINT Demo); Company Name: FayTechRemote Solutions Domain: faytechremotecareers.com Description: A fictional tech startup claiming to offer remote data entry jobs for European and African applicants. No verifiable company number, newly registered domain, no real employee profiles, and suspicious onboarding documents sent to applicants.

(II) Real/Legit Company (For Comparison); Company Name: Automattic, Inc. Domain: automattic.com Description: A real, reputable company that operates WordPress.com, Tumblr, WooCommerce, and more. Known for its strong remote-first culture, transparent hiring process, and well-documented online presence. This company will be used to show the contrast in digital footprint, transparency, and security posture compared to a scam.

1. OSINT TOOLS FOR DEEP TECHNICAL CONVERSATION

THESE ARE CORE TOOLS FOR UNCOVERING A COMPANY'S DIGITAL FOOTPRINT;

(I) THEHARVESTER;

This is an **OSINT** tool used to gather information about;

- Email addresses
- Domains & subdomains
- IPs and hosts
- Employee names (in some cases)

PS >> theHarvester does not have an official web GUI (Graphical User Interface), it only operates on CLI (Command Line Interface).

Command for usage >>

- This searches "faytechremotecareers.com" using Bing as the data source

```
theHarvester -d faytechremotecareers.com -b bing
```

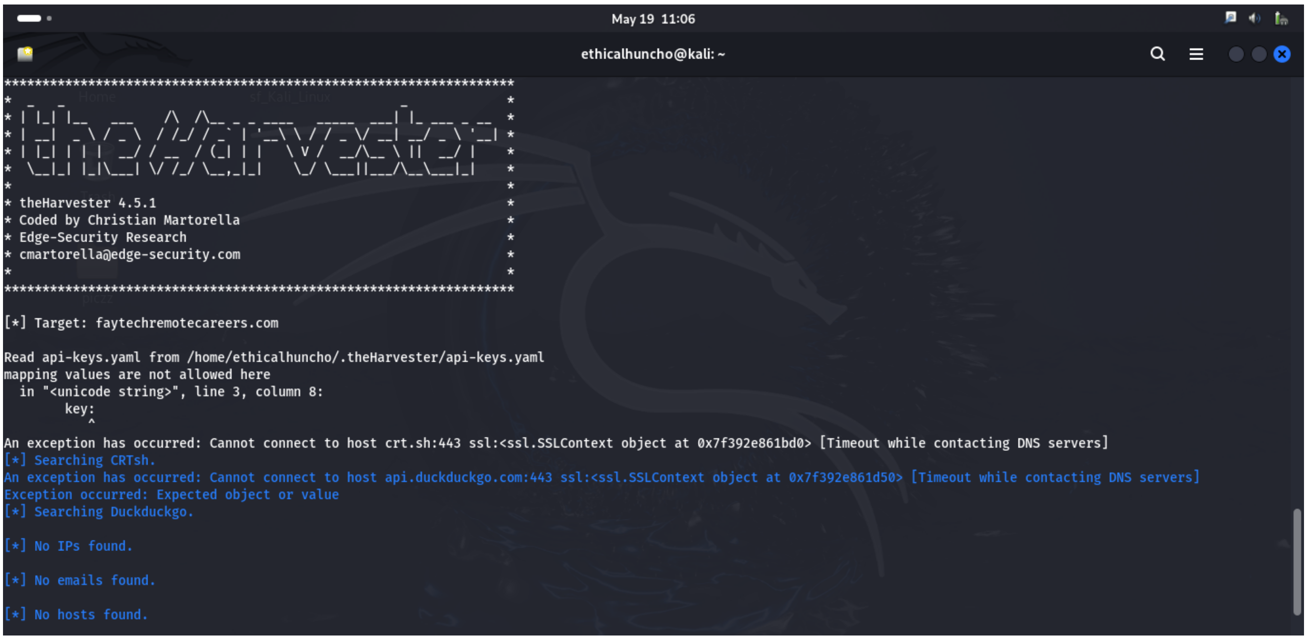
- This searches 'faytechremotecareers.com' using Bing as the data source

```
theHarvester -d faytechremotecareers.com -b duckduckgo
```

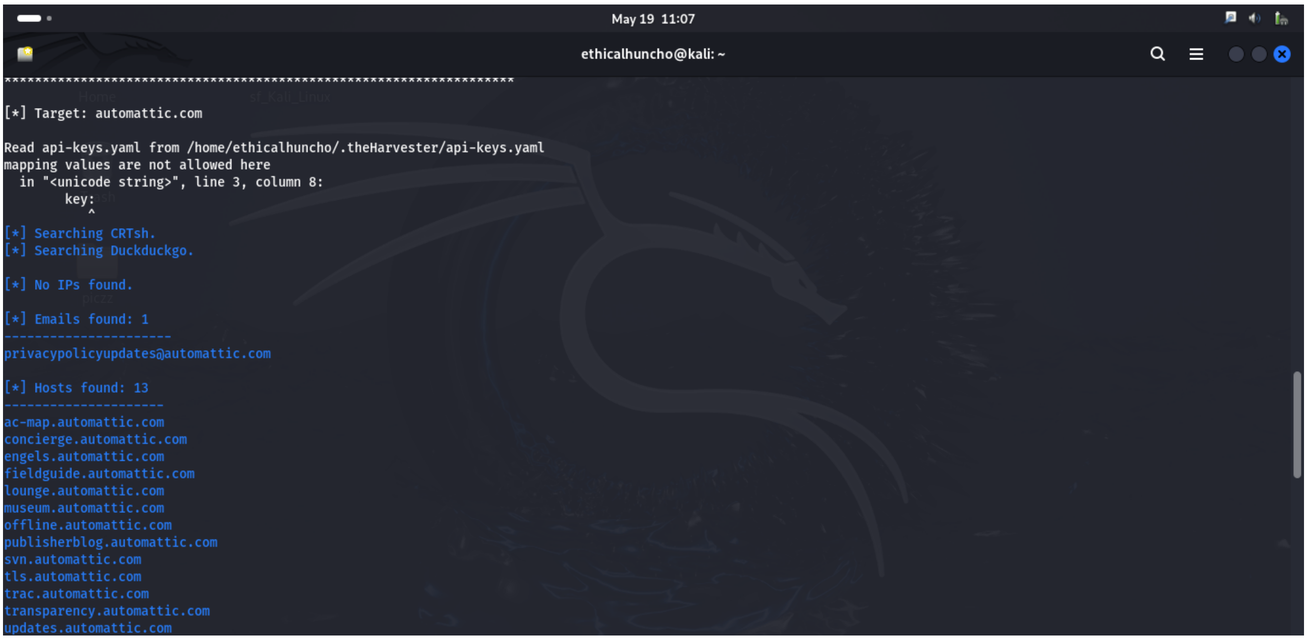
- This command tells theHarvester to use all available data sources (search engines/APIs) to collect information.

```
theHarvester -d faytechremotecareers.com -b all
```

The "all" includes sources like: Bing, Yahoo, DuckDuckGo, LinkedIn, Google (limited due to CAPTCHA issues), GitHub etc



```
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.5.1                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: faytechremotecareers.com

Read api-keys.yaml from /home/ethicalhuncho/.theHarvester/api-keys.yaml
mapping values are not allowed here
  in "<unicode string>", line 3, column 8:
        key:
           ^
An exception has occurred: Cannot connect to host crt.sh:443 ssl:<ssl.SSLContext object at 0x7f392e861bd0> [Timeout while contacting DNS servers]
[*] Searching CRTsh.
An exception has occurred: Cannot connect to host api.duckduckgo.com:443 ssl:<ssl.SSLContext object at 0x7f392e861d50> [Timeout while contacting DNS servers]
Exception occurred: Expected object or value
[*] Searching Duckduckgo.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```



```
*******************************************************************
[*] Target: automattic.com

Read api-keys.yaml from /home/ethicalhuncho/.theHarvester/api-keys.yaml
mapping values are not allowed here
  in "<unicode string>", line 3, column 8:
        key:
           ^
[*] Searching CRTsh.
[*] Searching Duckduckgo.

[*] No IPs found.

[*] Emails found: 1
----------------------
privacypolicyupdates@automattic.com

[*] Hosts found: 13
---------------------
ac-map.automattic.com
concierge.automattic.com
engels.automattic.com
fieldguide.automattic.com
lounge.automattic.com
museum.automattic.com
offline.automattic.com
publisherblog.automattic.com
svn.automattic.com
tls.automattic.com
trac.automattic.com
transparency.automattic.com
updates.automattic.com
```

The pictures above shows the clear difference between a real company and a fake one, it is impossible for a real hiring company not to have emails, subdomains, SSL Certs (CRT.sh), & DNS or IPs. Any scan that displays nothing is a red flag.

[Back to top]

(II) SPIDERFOOT;

Think of it like a spider that crawls the internet for clues about domains, IPs, emails, usernames etc

SpiderFoot automates the collection of OSINT data from over 200 data sources, including; WHOIS, DNS, Shodan, HaveIBeenPwned, Pastebin, Social media, Dark web resources (if configured) and more. This powerful tool has diverse functions, and it's highly used for multi-purpose reasons; Subdomain, DNS, IP address info, usernames, leaked credentials, emails exposed in breaching etc

PS; >> Unlike theHarvester, Spiderfoot offers both GUI and CLI.

INSTALLATION

```
 sudo apt install git python3 python3-pip -y (if already installed on your kali, no need for it again)
```

- **Clone the Spiderfoot Repository**

```
cd ~
git clone https://github.com/smicallef/spiderfoot.git
cd spiderfoot
```

- **Create a Virtual Environment**

```
sudo apt install python3-venv -y
python3 -m venv venv
source venv/bin/activate
```

- **Command for usage**

```
python3 sf.py -l 127.0.0.1:5001
```

Then open your browser and go to >> http://127.0.0.1:5001

(III) PHOTON;

This is a versatile OSINT tool designed for targeted web crawling and data extraction. It was created by **S0md3v**, Photon automates the process of extracting useful information from websites, which can then be used for any form of intel gathering.

INSTALLATION

```
sudo apt update
sudo apt install python3 python3-pip
git clone https://github.com/s0md3v/Photon.git
```

```
cd Photon
pip3 install -r requirements.txt
```

- **Command for usage >>**

```
python3 photon.py -u faytechremotecareers.com -l 2
```

This command will crawl the website "faytechremotecareers.com", and gathers a few information like IP's, emails or any leaks pertaining to the company.

[Back to top]

(IV) HOLEHE;

Developed and built by **Megadose**, **Holehe** is an OSINT tool that lets you check if a particular email address is associated with accounts on popular online platforms and services (Spotify, Twitter, Adobe, Github etc). It’s useful for footprinting during an investigation, red teaming, or digital forensics. It’s useful in reconnaissance and enumeration phases of ethical hacking or threat intelligence investigations, especially for;

- Footprinting individuals or companies
- Credential leak analysis
- Detecting reused emails across platforms

INSTALLATION

```
sudo apt update
sudo apt install python3 python3-pip
pipx install holehe
```

- **Command for usage >>**

```
holehe faytechremotecareers.com
```

(V) RECON-NG

Recon-ng is a full-featured reconnaissance framework, developed by **Tim Tomes**, written in Python. It's designed to conduct web-based open-source intelligence (OSINT) gathering in a modular, scriptable, and automatable environment. Think of it as a Swiss army knife for reconnaissance, allowing you to gather emails, subdomains, hosts, credentials, and more from public sources.

INSTALLATION

```
sudo apt update
sudo apt install recon-ng -y
```

Command for usage >>

- Run the console

```
recon-ng
```

- Create a Workspace (Workspaces allow you to separate recon projects)

```
workspaces create faytechremotecareers
```

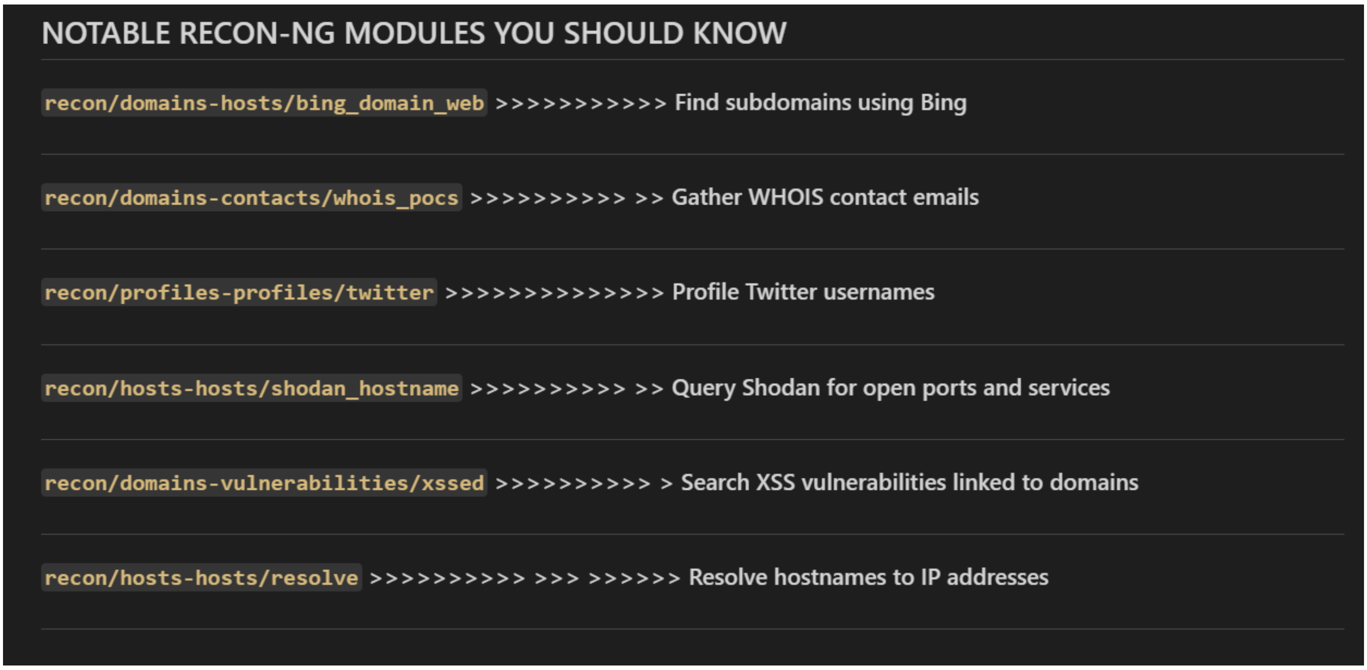
- Add a Domain (This will search Bing for hosts related to faytechremotecareers.com)

```
modules load recon/domains-hosts/bing_domain_web
options set DOMAIN faytechremotecareers.com
options show
run
```

- View Results

```
show hosts
```

[Back to top]



NOTABLE RECON-NG MODULES YOU SHOULD KNOW

`recon/domains-hosts/bing_domain_web` >>>>>>>>>>> Find subdomains using Bing

`recon/domains-contacts/whois_pocs` >>>>>>>>>> >> Gather WHOIS contact emails

`recon/profiles-profiles/twitter` >>>>>>>>>>>>>> Profile Twitter usernames

`recon/hosts-hosts/shodan_hostname` >>>>>>>>>> >> Query Shodan for open ports and services

`recon/domains-vulnerabilities/xssed` >>>>>>>>>> > Search XSS vulnerabilities linked to domains

`recon/hosts-hosts/resolve` >>>>>>>>>> >>> >>>>>> Resolve hostnames to IP addresses

- View Available API Keys

```
keys list
```

- Add an API Key

```
keys add <key_name> <api_key_value>
```

EXAMPLE, SHODAN >>

```
keys add shodan_api XyZ123YourShodanAPIKeyHere
```

EXAMPLE, TWITTER >>

```
keys add twitter_api XYZ456YourTwitterKeyHere
keys add twitter_api_secret YourSecretHere
```

- Verify It's Added

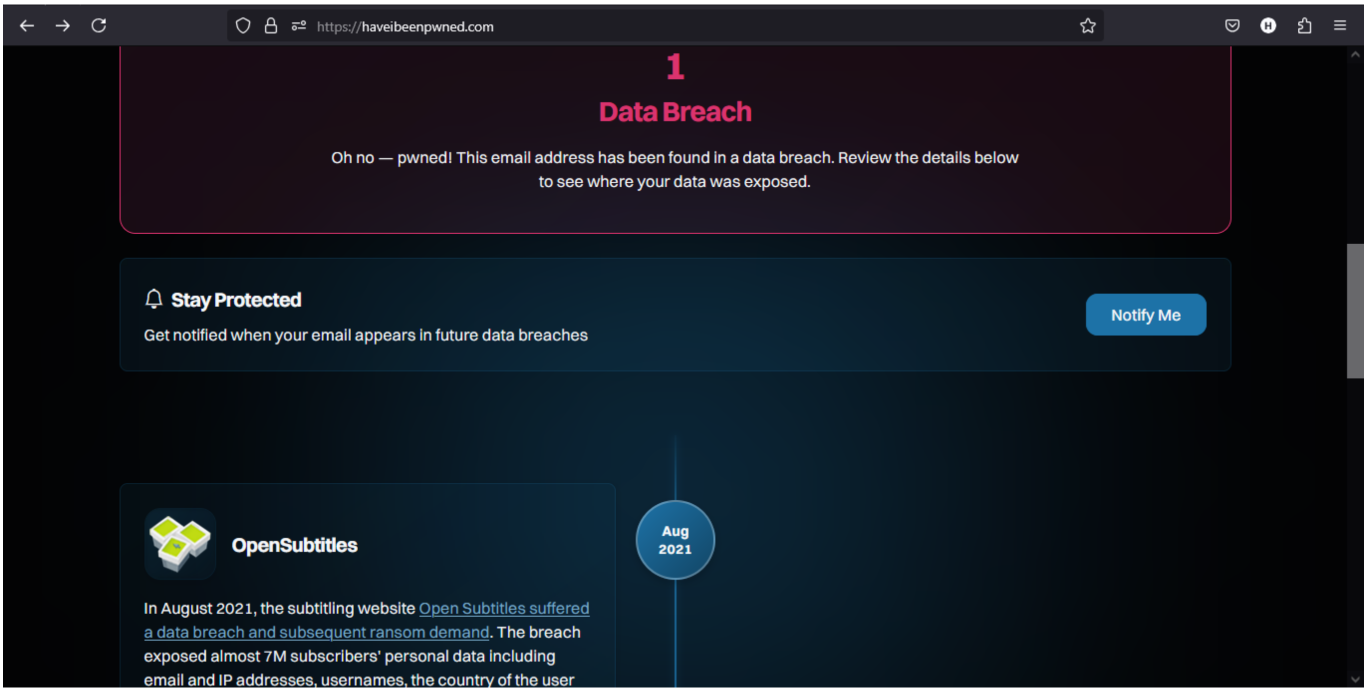
```
keys list
```

(VI) HAVEIBEENPAWNED

HaveIBeenPwned is a widely used OSINT tool that helps identify if personal data, especially email addresses, usernames, and passwords, have been compromised in data breaches. It is incredibly useful in cybersecurity investigations, digital footprinting, threat intelligence, and due diligence.

USES

- Checks if an email address, phone number, or domain has appeared in public data breaches
- Provides breach details (what was leaked, when, which service)
- Has a Pwned Passwords service to check if a password is already known publicly



1

Data Breach

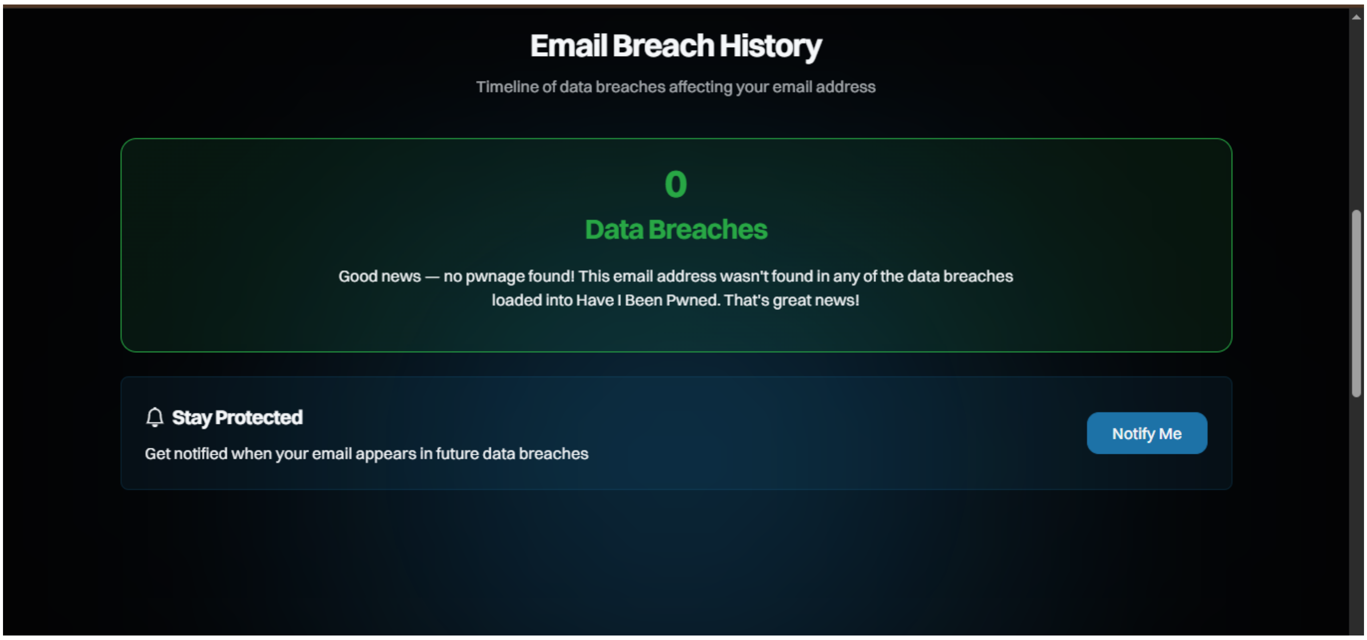
Oh no — pwned! This email address has been found in a data breach. Review the details below to see where your data was exposed.

Stay Protected

Get notified when your email appears in future data breaches

OpenSubtitles

In August 2021, the subtitling website Open Subtitles suffered a data breach and subsequent ransom demand. The breach exposed almost 7M subscribers' personal data including email and IP addresses, usernames, the country of the user



Email Breach History

Timeline of data breaches affecting your email address

0

Data Breaches

Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!

Stay Protected

Get notified when your email appears in future data breaches

The above screenshots illustrate the differentiation between email addresses that have appeared in known data breaches and those that remain uncompromised. For every breached record identified, details regarding the affected platforms and breach incidents will be incorporated into the report. This

enhances the tool's value for credential exposure analysis and incident tracking.

[Back to top]

2. SOCIAL MEDIA + PEOPLE SEARCH TOOLS

THESE TOOLS CAN BE USED TO VALIDATE RECRUITERS, EMPLOYEE CLAIMS, COMPANY ACTIVITIES;

(I) LINKEDIN

LinkedIn, owned by Microsoft, is the world's largest professional social networking platform. Recent studies has shown that LinkedIn boasts over 1 billion users globally, making it a goldmine for;

- Career progression
- Business networking
- Corporate intelligence
- OSINT recon

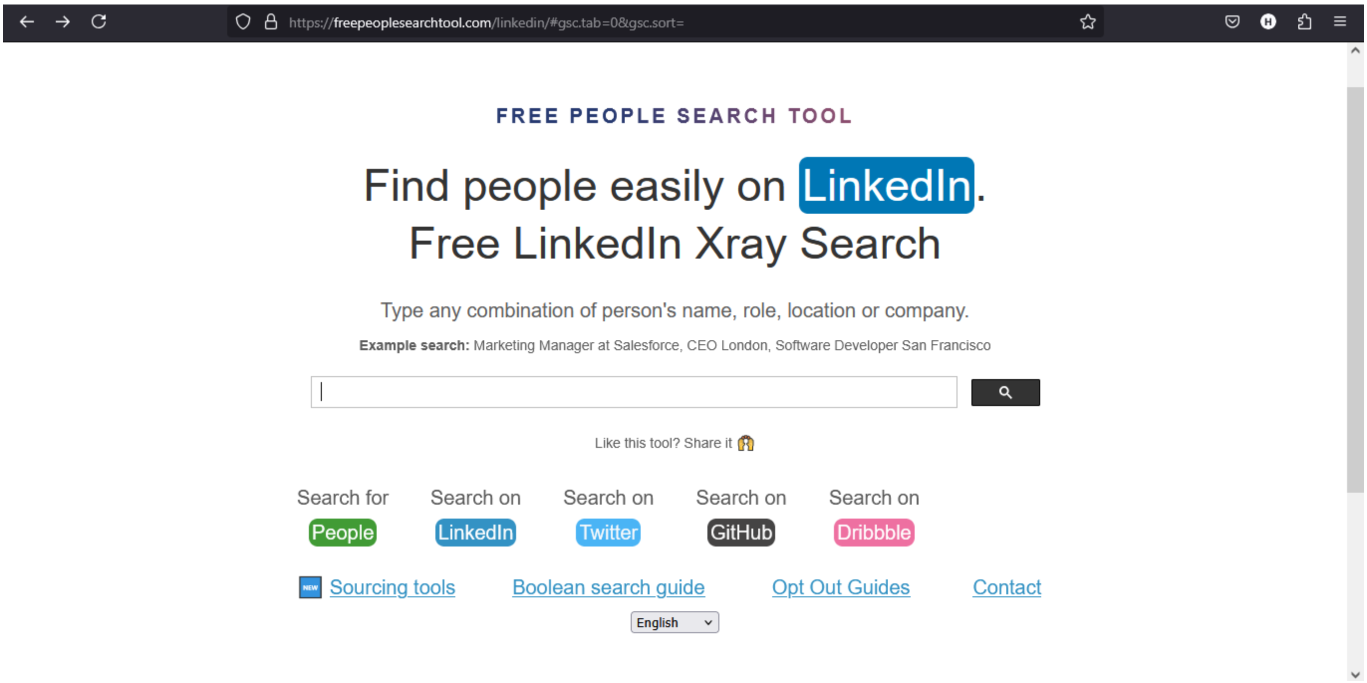
WHAT YOU CAN DO ON LINKEDIN (INVESTIGATION & OSINT PURPOSES)

- Gather public professional information
- Trace job origins
- Harvest emails, if already exposed
- Identify company executives & decision makers
- Thoroughly checking of; profiles, job posts, comments, associates, connections & whole network.

Some reconnaissance techniques shared on LinkedIn are also applicable to platforms like TWITTER/X and FACEBOOK.

(II) FREEPEOPLESEACRHTOOL

FreePeopleSearchTool.com, is an online people search engine aggregator. It is designed to pull publicly available data and indexed records about individuals from various open-source or semi-public databases across the web (LinkedIn, Facebook etc). Basically, you input a name, phone number, email, or location, and it returns whatever publicly accessible intel it can find associated with that query.



https://freepeoplesearchtool.com/linkedin/#gsc.tab=0&gsc.sort=

FREE PEOPLE SEARCH TOOL

Find people easily on LinkedIn.
Free LinkedIn Xray Search

Type any combination of person's name, role, location or company.

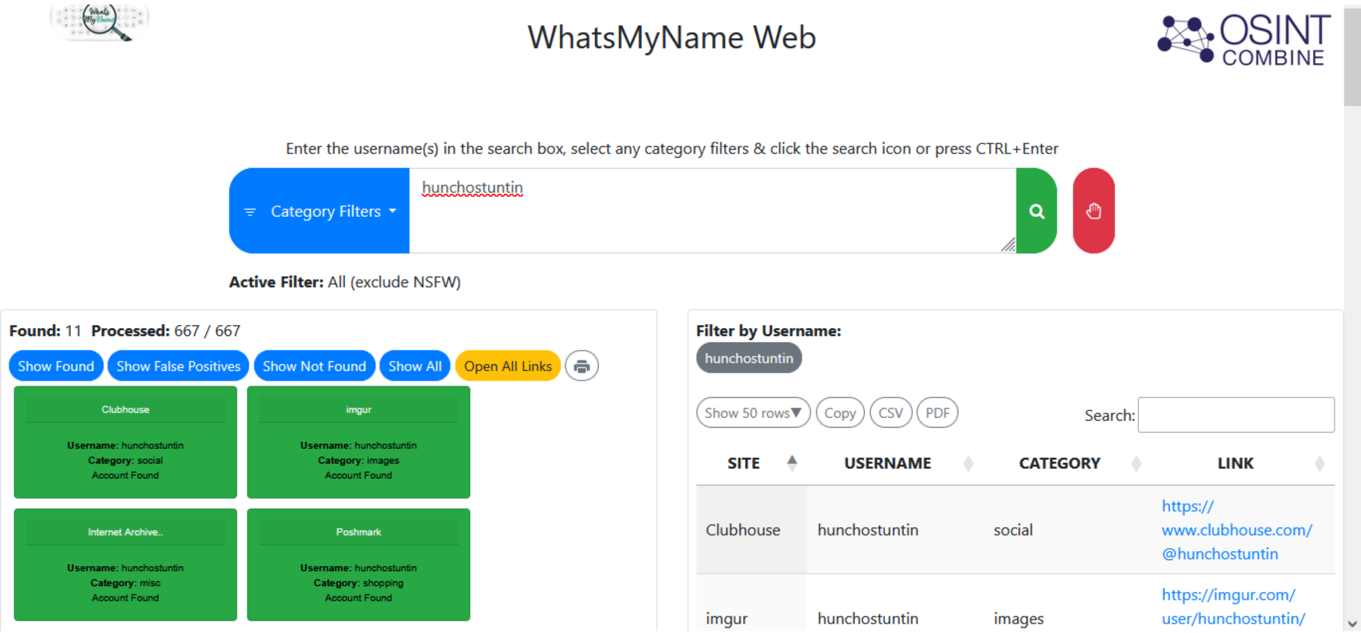
Example search: Marketing Manager at Salesforce, CEO London, Software Developer San Francisco

(III) WHATSMYNAME

WhatsMyName is a powerful OSINT tool, discovered by WebBreacher, focused on username enumeration across hundreds of websites and services. It helps investigators, penetration testers, and OSINT researchers track a digital footprint by checking if a specific username is in use on various platforms; social media, gaming sites, coding platforms, etc.

OSINT USE CASES

- Checks if a username exists on 500+ services (social media, forums, dating sites, crypto markets)
- Can be paired with Photon, **Holehe, Maigret,** and **Recon-ng** workflows
- Building digital footprints for missing persons or Cyberstalking investigations
- Verifying aliases for fraud or identity theft inquiries



WhatsMyName Web

Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter

hunchostuntin

Active Filter: All (exclude NSFW)

Found: 11 **Processed:** 667 / 667

Clubhouse
Username: hunchostuntin
Category: social
Account Found

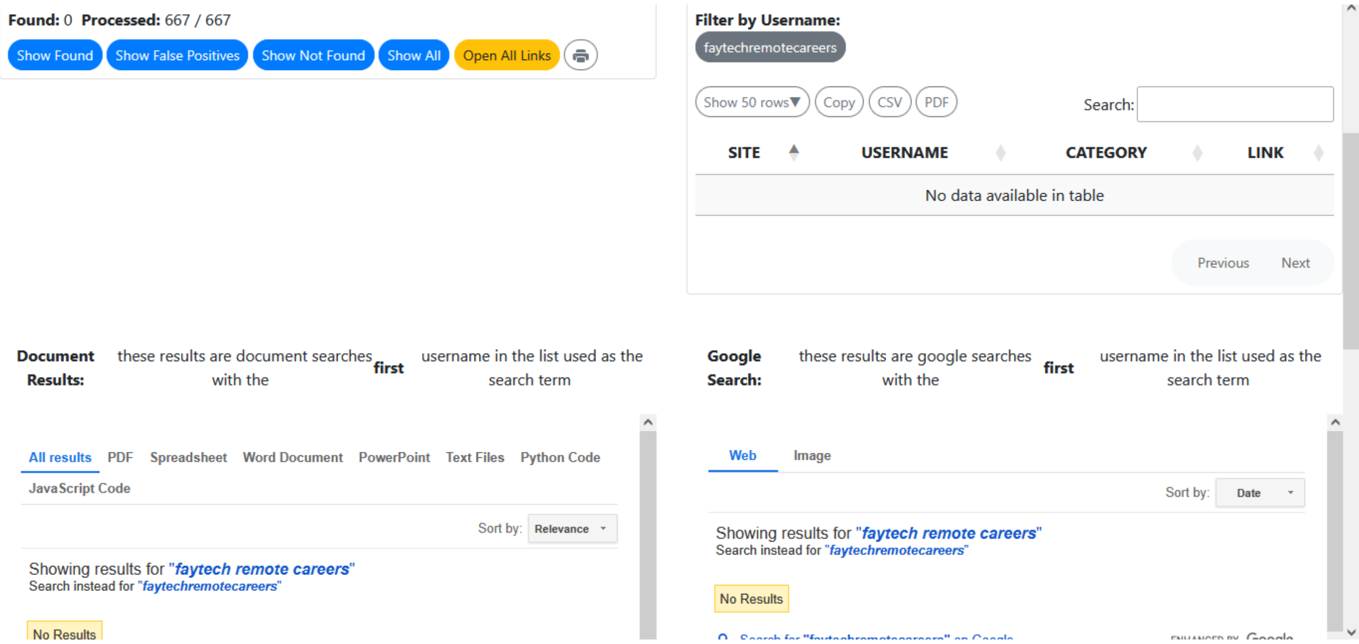
imgur
Username: hunchostuntin
Category: images
Account Found

Internet Archive..
Username: hunchostuntin
Category: misc
Account Found

Poshmark
Username: hunchostuntin
Category: shopping
Account Found

Filter by Username:
hunchostuntin

SITE	USERNAME	CATEGORY	LINK
Clubhouse	hunchostuntin	social	https://www.clubhouse.com/@hunchostuntin
imgur	hunchostuntin	images	https://imgur.com/user/hunchostuntin/



Found: 0 **Processed:** 667 / 667

Filter by Username: faytechremotecareers

Search:

SITE	USERNAME	CATEGORY	LINK
No data available in table			

Document Results: these results are document searches with the **first** username in the list used as the search term

Google Search: these results are google searches with the **first** username in the list used as the search term

Sort by: Relevance

Showing results for "*faytech remote careers*"
Search instead for "*faytechremotecareers*"

No Results

Sort by: Date

Showing results for "*faytech remote careers*"
Search instead for "*faytechremotecareers*"

No Results

Getting a "no result or no data available" after running a scan on a prospective employer or company might be a red flag, reputable & real companies always have digital footprints, regardless of its establishment date.

[Back to top]

(IV) GOOGLE DORKING

Google Dorking involves using advanced search operators to refine Google search queries, and uncover specific file types, sensitive directories, credentials, error messages, or exposed assets that are not visible through ordinary browsing. These operators enable professionals to dig deeper into indexed web content than the average user.

Google Dorking is used during reconnaissance and due diligence to;

- Discover exposed files
- Identify vulnerable systems
- Uncover forgotten subdomains
- Spot leaked credentials or emails

CORE GOOGLE DORKING OPERATORS WITH EXAMPLES;

1. SITE

Limits results to a specific website or domain

- *Example 1 (Finds LinkedIn profiles or pages mentioning cybersecurity analyst)*

```
site:linkedin.com "cybersecurity analyst"
```

- *Example 2 (Shows all pages from Automattic's site that mention the word privacy)*

```
site:automattic.com privacy
```

2. INURL

Detect some specific paths and sensitive pages (e.g., login, admin pages)

- *Example 1 (Lists pages with “login” in their address e.g., admin login panels)*

```
inurl:login
```

- *Example 2 (Searches for .gov.in sites with "password" in their URL)*

```
site:gov.in inurl:password
```

3. INTITLE

Identify pages with specific labels or headers (what appears in browser tabs or search result titles)

- *Example 1 (Finds open directory listings related to “confidential")*

```
intitle:"index of" confidential
```

- *Example 2 (Looks for login-related pages on Facebook)*

```
intitle:login site:facebook.com
```

4. FILETYPE

Searches for specific file types (e.g. docx, configs, xls, pdf)

- *Example 1 (Looks for PDF documents on the WHO site related to climate change.)*

```
filetype:pdf site:who.int "climate change"
```

5. CACHE

View Google’s cached version of a site

- *Example 1 (Shows the last cached version of faytechremotecareers homepage)*

```
cache:faytechremotecareers.com
```

- *Example 2 (Opens Google’s stored copy of that login page)*

```
cache: faytechremotecareers.com/login
```

[Back to top]

6. INTEXT

Finds a word or phrase inside the content (body) of web pages, digs into the actual content of a page

- *Example 1 (Finds pages containing the phrase "internal use only")*

```
intext:"internal use only"
```

- *Example 2 (Searches PDF files that contain the word "SSN" (Social Security Number))*

```
intext:"SSN" filetype:pdf
```

7. BOOLEAN LOGIC & FILTERS IN GOOGLE DORKING [`OR` / `AND` / `-` / `"`]

Boolean logic helps refine Google searches using logical operators like `OR`, `AND`, `-`, and `"  "`. They tell Google exactly what you want, and more importantly, what you don’t want. Helps find useful, often hidden, information.

A. `"  "` Exact Phrase Searching

Finds only results with that exact phrase or term, Spotting leaked or misconfigured files.

- *Example 1 (Finds pages with the exact phrase "login page", not just “login” or “page” separately)*

```
"login page"
```

- *Example 2 (Lists documents and pages with that specific internal notice)*

```
"internal use only"
```

B. `OR` Either One

Finds pages that match one OR the other of two or more keywords. It finds profiles/pages that use different terms for the same thing, it broadens scope during recon (e.g., aliases or role variations).

- *Example 1 (Find pages with either 'admin login' or 'dashboard login')*

```
"admin login" OR "dashboard login"
```

- *Example 2 (Useful for people enumeration, matches either term)*

```
site:linkedin.com "penetration tester" OR "bug bounty"
```

C. `AND` — Both Must Appear (implicitly used)

Google includes all words by default, but you can still use AND for clarity.

- *Example (Finds ".pdf" files on ".gov" sites that include "climate change")*

```
site:gov filetype:pdf AND "climate change"
```

D. `-` (Minus Sign) — Exclude a Word

Its purpose is to exclude specific words or domains from results. Excludes; marketing pages, FAQs, or directories from intel gathering.

- *Example (Shows results from faytechremotecareers.com, but excludes any page with "login" in it)*

```
site:faytechremotecareers.com -login
```

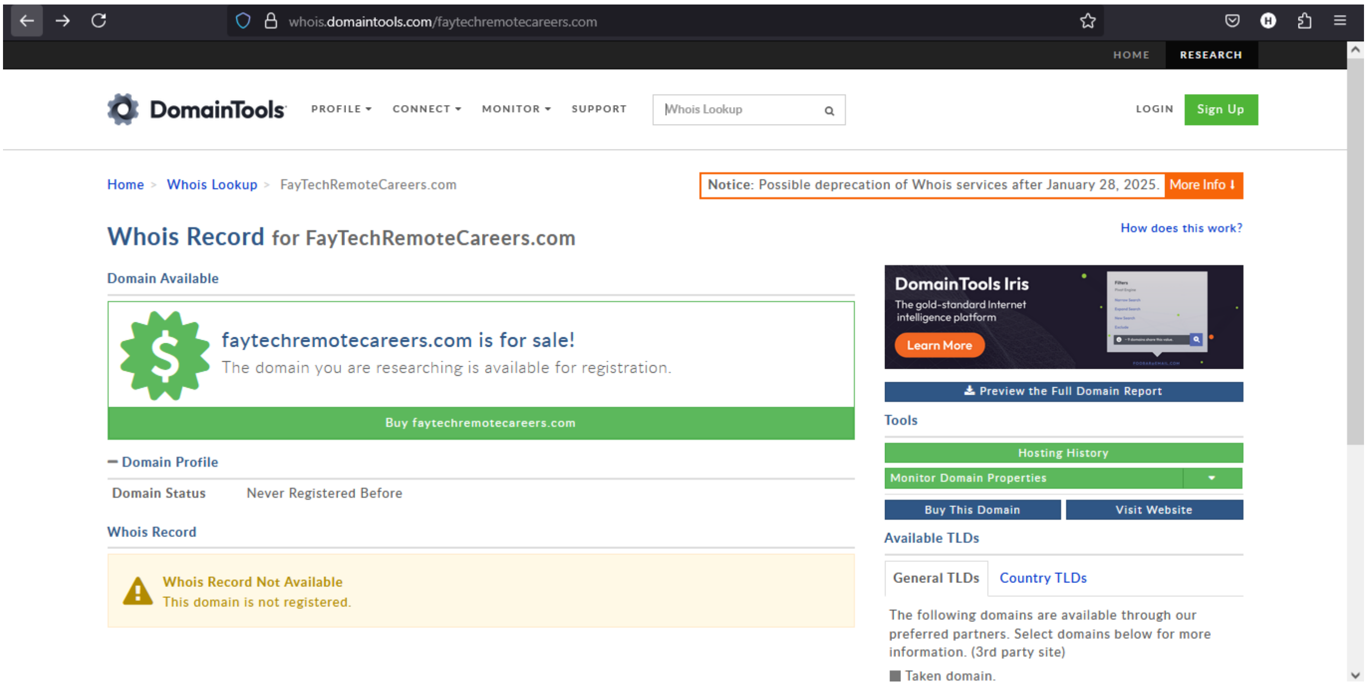
[Back to top]

3. Domain & Company Identity Verification

Domain and Company Identity Verification is the process of confirming the authenticity and ownership of an internet domain, and ensuring that a company is legitimate, and credible.

WHOIS LOOKUP

Whoisdomaintools & Whois Reveals ownership, registration info, domain age, creation&expiry dates, Check when domain was registered


whois.domaintools.com/faytechremotecareers.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Home > Whois Lookup > FayTechRemoteCareers.com
More Info
How does this work?
DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Buy This Domain
Visit Website
Available TLDs
General TLDs
Country TLDs
Buy faytechremotecareers.com

Notice: Possible deprecation of Whois services after January 28, 2025.

Whois Record for FayTechRemoteCareers.com

Domain Available

faytechremotecareers.com is for sale!
The domain you are researching is available for registration.

Domain Profile

Domain Status: Never Registered Before

Whois Record

Whois Record Not Available
This domain is not registered.

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

■ Taken domain.

A non-registered domain might be a red flag to remote job seekers, a real & legitimate company will have a registered domain, and the search will respond with domain name registration and every other important details.

[Back to top]

IN AN AGE WHERE REMOTE WORK IS THE NORM, DISTINGUISHING BETWEEN GENUINE OPPORTUNITIES AND DECEPTIVE TRAPS IS MORE IMPORTANT THAN EVER. THROUGH THIS INVESTIGATION, WE'VE SEEN HOW OSINT TOOLS CAN UNCOVER DIGITAL FOOTPRINTS AND SUPPORT INFORMED DECISION-MAKING. FROM VERIFYING DOMAINS TO ANALYZING COMPANY CREDIBILITY, THESE TECHNIQUES EMPOWER JOB SEEKERS AND ANALYSTS ALIKE. WITH THE RIGHT MINDSET AND TOOLS, DUE DILIGENCE CAN BECOME SECOND NATURE, HELPING US STAY SAFE AND AWARE IN AN INCREASINGLY DIGITAL JOB MARKET.