

Public Breached Search | Public Breaches (140+ Billion Records)

Public Breached Search

Attention: The search is performed on a large aggregated database of public leaks on the Internet (>140B records / 4500+ sources). Use only to verify your data or with explicit permission (abuse of the service will result in account suspension). Some results may contain outdated or inaccurate information. Publication of data obtained on this page in the public domain is prohibited. If you encounter search errors, delete one character from your query and repeat the search. **Search is available only with a subscription.**

Search in Leaks

Email / Login / Domain / Phone / IP / URL / Combo

Summary JSON CSV Raw

QUERY (EX: EXAMPLE@MAIL.COM / @GMAIL.COM / NICKNAME / +09001234567 / DOMAIN.COM / EMAIL PASS / FULL NAME / NAME CITY / SOCIAL NETWORK ID ...):

example@mail.com / @gmail.com / nickname / +09001234567 / domain.com / email pass /

Search

Reset

Examples of Queries::

Email Domain Emails Username Phone Email+Pass Name+Phone

Minimum interval between requests: **10 seconds** (anti-spam).

Description

The tool aggregates results from multiple public leaks available on the internet and displays structured data blocks (email, hashes, IP, profiles, activity dates, etc.).

- Up to 140B lines
- 4500+ sources
- Risk Indicator
- Caching Results
- Export CSV
- Data is protected by Cryptography

Use ethically. Change passwords if compromise is detected. If abuse of the service is detected, the account will be disabled and blocked.

Request History

Filter... Clear

Only parameters and aggregated metadata (without confidential strings) are stored in the history.

Tips:

Combined search: email + password / name + phone number, etc.
Passwords/hashes masked until clicked.
Groups - individual records/field combinations in the source.
Cooldown: 10s - anti-spam.
Bank Cards and Medical Data: are automatically removed from indexes and are not available for search.
Export displays structures without sensitive fields disclosed.
Incorrect result? The search engine searches through a large amount of data. Repeat the search by removing one character from the query.
Indexation: didn't get a result from the system? Try again later. The system indexes public sources, and the result will most likely be available in the future.

Overview of the Service

The platform available at dash.niamonx.io/breaches_search is a professional-grade **Public Breached Data Search System** designed for verifying whether specific personal identifiers have appeared in any known public data leaks across the Internet.

It operates on an **aggregated dataset exceeding 140 billion records** collected from **over 4,500 public breach sources**, making it one of the most extensive publicly searchable breach databases in existence.

? How the Search Works

When a user enters a query — such as an **email address, username, phone number, IP, or domain** — the system performs a real-time lookup across its encrypted, indexed data clusters. The query is normalized, tokenized, and securely matched against hashed or pseudonymized datasets to locate potential breach entries.

The search engine uses **multi-vector indexing** optimized for text, numeric, and composite keys (e.g., *email + password*, *name + city*), allowing flexible combined searches.

To maintain integrity and performance:

- Each user request is subject to a **10-second cooldown** (anti-spam policy).
 - Partial queries can improve recall; deleting one character may trigger a broader match.
 - Cached results are used for frequent queries to improve response time.
-

? What Can Be Searched

You can look up:

- **Emails and logins**
- **Phone numbers** (international format)
- **Domains or URLs**
- **IP addresses**
- **Full names or social network identifiers**
- **“Combo” lines** (e.g., *email + password* pairs from public leaks)

The system structures results into logical “groups” that may include:

- Email or login identifiers
- Hashed or masked passwords
- IP and domain references
- Profiles and related metadata
- First/last seen activity dates

Sensitive fields like passwords remain **masked** until explicitly revealed by the user.

?? Security & Ethics

All stored data and query logs are **encrypted using modern cryptographic algorithms**. Only **aggregated metadata** — not full confidential strings — is retained in request history for transparency and analytics.

Additional safeguards:

- **Bank card and medical information** are automatically excluded from indexing.
- **Publication of retrieved data** is strictly forbidden.
- Detected abuse leads to **account suspension and IP blocking**.

The service is intended for **ethical use only** — such as checking whether your credentials or company assets appear in public leaks and taking appropriate security measures (e.g., password changes, MFA setup).

? Extra Features

- **Risk indicator:** assesses the exposure level of each result.
 - **Result caching:** speeds up repeated lookups.
 - **CSV export:** allows structured export without revealing sensitive fields.
 - **Ongoing index updates:** new sources are continuously crawled and normalized.
-

In summary, **NiamonX Breach Search** acts as a secure, encrypted intelligence platform that enables professionals and individuals to verify their exposure in public breaches responsibly. It prioritizes **data protection, cryptographic integrity, and ethical transparency**, providing actionable insights while maintaining user and data privacy.

? Contact Information

For any inquiries, users can contact the project team directly:

- [support @ niamonx.io](mailto:support@niamonx.io) — Technical Support
- [other @ niamonx.io](mailto:other@niamonx.io) — General Inquiries
- [takedown @ niamonx.io](mailto:takedown@niamonx.io) — Requests for Data Removal / Privacy Takedowns
- [legal @ niamonx.io](mailto:legal@niamonx.io) — Legal Matters

An alternative contact channel is the official **Helpdesk**:

📄 <https://support.niamonx.io/>

Revision #3

Created 9 November 2025 05:08:26 by NiamonX Team

Updated 9 November 2025 05:27:44 by NiamonX Team