

# Dov'è finito il mio indirizzo email?

Questo esercizio mira a far conoscere uno strumento, come ne esistono diversi, per consultare rapidamente più data breach pubblici. Questi strumenti avevano più senso in un mondo pre-GDPR, perchè ora le aziende sono obbligate legalmente a notificare gli utenti nel caso i loro dati venissero compromessi. Tuttavia, il primo passo che un'azienda ha per poter denunciare queste compromissioni, è scoprirle, il secondo è capirne l'estensione e infine denunciarle: purtroppo sono rari i casi in cui sussistano tutti e tre, ed è bene che l'utente tenga questo a mente.

## Per chi?

Per tutte le persone che dispongono di un account su un qualsiasi provider di servizi online

## Durata

Qualche minuto

## Livelli arcobaleno + tag/keyword

(principale)

L3, data warehousing, third party data sharing

(secondari)

L1, Locard

## Difficoltà (relativa all'utente)

Facile

## Strumenti necessari

- Un indirizzo email
- Un qualsiasi browser su un qualsiasi sistema operativo
- Conoscenza di base dell'inglese

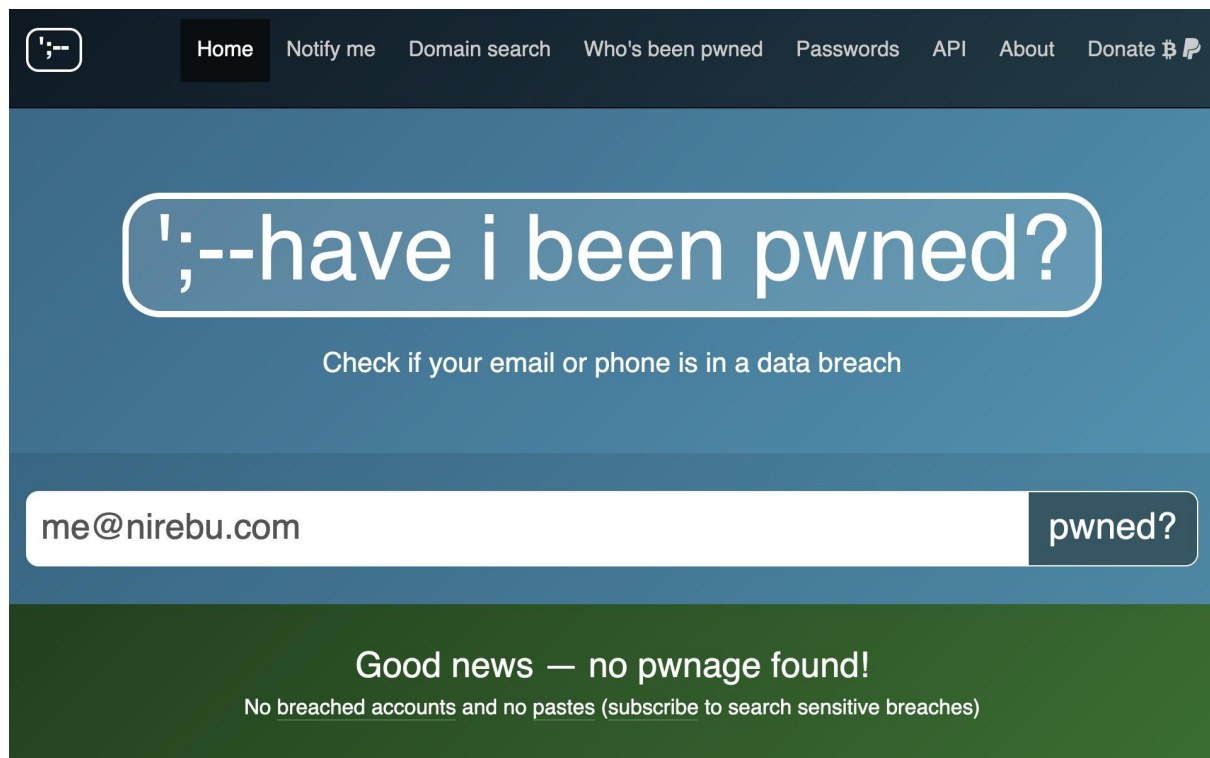
## Costi

0

## Istruzioni dettagliate

- Visitare il sito web <https://haveibeenpwned.com/>
- Inserire un proprio indirizzo email o numero di telefono nel campo di ricerca
- Avviare la ricerca

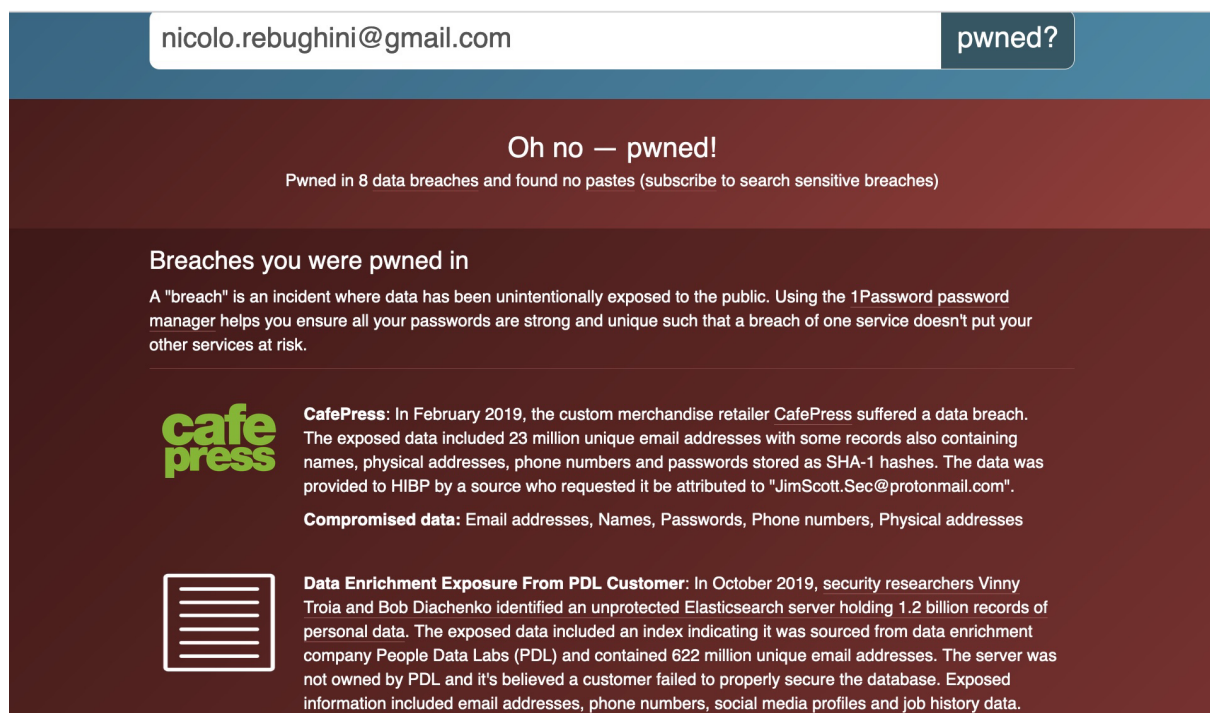
## Risultati attesi



The screenshot shows the homepage of the 'have i been pwned?' website. The navigation bar at the top includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is 'have i been pwned?' with a subtitle 'Check if your email or phone is in a data breach'. A search input field contains 'me@nirebu.com' and a button labeled 'pwned?'. Below the search bar, a green banner displays the message 'Good news — no pwnage found!' followed by the text 'No breached accounts and no pastes (subscribe to search sensitive breaches)'.

Il risultato ideale è che il proprio identificativo inserito non sia presente in nessun data breach di cui sono pubblici i dati. Se il proprio identificativo è invece presente, ci sarà a disposizione l'elenco dei provider da cui questi dati sono stati estrapolati.

## Lessons learned / Obiettivi



The screenshot shows the search results page for 'nicolo.rebughini@gmail.com'. The search bar at the top shows the email address and a 'pwned?' button. The main heading is 'Oh no — pwned!' with the subtitle 'Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)'. Below this, a section titled 'Breaches you were pwned in' provides details about the breaches. The first breach is 'CafePress', which occurred in February 2019, exposing 23 million unique email addresses and other personal data. The second breach is 'Data Enrichment Exposure From PDL Customer', which occurred in October 2019, exposing 622 million unique email addresses and other personal data.

**Breaches you were pwned in**

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

**cafe press** **CafePress:** In February 2019, the custom merchandise retailer CafePress suffered a data breach. The exposed data included 23 million unique email addresses with some records also containing names, physical addresses, phone numbers and passwords stored as SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Compromised data:** Email addresses, Names, Passwords, Phone numbers, Physical addresses

**Data Enrichment Exposure From PDL Customer:** In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Vedendo il proprio indirizzo email comparire in diversi data breach (come nel caso riportato nello screenshot) l'utente dovrebbe risultare più sensibile di fronte alla scelta di “consegnare” i propri dati identificativi a terzi.

## Possibili mitigazioni

Uno strumento che i maggiori email provider offrono che può aiutarci a “moltiplicare” i nostri indirizzi email in modo da, sia renderli più unici e marginalmente meno utili nel caso di un breach, sia per capire chi ha accidentalmente perso i nostri dati. Ad esempio, se il nostro indirizzo gmail è “[nomeutente@gmail.com](#)”, noi possiamo registrarci a servizi specifici utilizzando un'email specifica per quello, come ad esempio “[nomeutente+ebay@gmail.com](#)”. In questo modo riceveremo comunque i messaggi nella nostra casella, ma se troviamo questo indirizzo in un data breach, potremo essere quasi certi che esso è avvenuto presso quel provider specifico su cui abbiamo utilizzato quello specifico indirizzo, o che il dato sia stato venduto a terze parti e poi esposto al pubblico.

## Proseguì con...

Il servizio offre anche la possibilità di controllare se una propria password è stata identificata in un data breach e crackata con successo. È presente anche una sezione che dettaglia i data breach avvenuti e le aziende coinvolte.

## Licenza

CC-BY