

OSINT Industries

Report for: **CHARLES.GABI@GMAIL.COM**

As of **2025-08-23T00:36:39.832Z**

[Map](#) • [Modules](#) • [Timeline](#)

Module Responses

FACEBOOK

Registered : true

Email Hint : c*****a@gmail.com

LINKEDIN

Registered : true

Id : urn:li:person:DgFHHXVrbntLx7myubKOnxIsFFIl1YKJTCZ-UnusjsI

Name : Gabi Karl

First Name : Gabi

Last Name : Karl

Language : en (us)

Location : Portland, Oregon, United States

Username : gabi-karl-3533807a

Profile Url : https://linkedin.com/in/gabi-karl-3533807a

Bio : Health, Wellness and Fitness Professional

Private : false

HIBP

Registered : true

Breach : true

Name : Adobe

Website : adobe.com

Bio : In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also [disclosed much about the passwords](http://www.troyhunt.com/2013/11/adobe-credentials-and-serious.html) adding further to the risk that hundreds of millions of Adobe customers already faced.

Creation Date : 2013-10-04T00:00:00



Registered : true

Breach : true

Name : Verifications.io

Website : verifications.io

Bio : In February 2019, the email address validation service [verifications.io](https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service) suffered a data breach. Discovered by [Bob Diachenko](https://twitter.com/mayhemdayone) and [Vinny Troia](https://twitter.com/vinnytroia), the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although [an archived copy remains viewable](https://web.archive.org/web/20190227230352/https://verifications.io/).

Creation Date : 2019-02-25T00:00:00





Registered : true

Breach : true

Name : Evite

Website : evite.com

Bio : In April 2019, the social planning website for managing online invitations <a

href="https://www.evite.com/security/update?

usource=lc<id=1800182" target="_blank"

rel="noopener">Evite identified a data breach of their

systems. Upon investigation, they found unauthorised

access to a database archive dating back to 2013. The

exposed data included a total of 101 million unique email

addresses, most belonging to recipients of invitations.

Members of the service also had names, phone numbers,

physical addresses, dates of birth, genders and passwords

stored in plain text exposed.

Creation Date : 2013-08-11T00:00:00

Registered : true

Breach : true

Name : Data Enrichment Exposure From PDL Customer

Bio : In October 2019, <a

href="https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses"

target="_blank" rel="noopener">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.

Creation Date : 2019-10-16T00:00:00



Registered : true

Breach : true

Name : Chatbooks

Website : chatbooks.com

Bio : In March 2020, the photo print service Chatbooks suffered a data breach which was subsequently put up for sale on a dark web marketplace. The breach contained 15 million user records with 2.5 million unique email addresses alongside names, phone numbers, social media profiles and salted SHA-512 password hashes. The data was provided to HIBP by dehashed.com.

Creation Date : 2020-03-26T00:00:00

Registered : true

Breach : true

Name : Cit0day

Website : cit0day.in

Bio : In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Creation Date : 2020-11-04T00:00:00

PINTEREST

Registered : true

EVENTBRITE

Registered : true

Id : 177933594019

Verified : false

GOODREADS

Registered : true

Id : 64843619

Name : Gabriela Karl

Profile Url :

<https://www.goodreads.com/user/show/64843619-gabriela-karl>



NEXTDOOR

Registered : true

DISQUS

Registered : true

Timeline

Content: Breached on Adobe

Date/Year: 2013-10-04T00:00:00

Content: Breached on Verifications.io

Date/Year: 2019-02-25T00:00:00

Content: Breached on Evite

Date/Year: 2013-08-11T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer

Date/Year: 2019-10-16T00:00:00

Content: Breached on Chatbooks

Date/Year: 2020-03-26T00:00:00

Content: Breached on Cit0day

Date/Year: 2020-11-04T00:00:00

[osint.industries](https://app.osint.industries)