

OSINT Industries

Report for: **kingscolony7123@yahoo.com**

As of **2024-09-25T01:38:38.936Z**

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

Module Responses

GOOGLE

Registered : true

Id : 108050409165180930563

Last Seen : 2023-03-26T00:14:34



MYFITNESSPAL

Registered : true

HIBP

Registered : true

Breach : true

Name : 8fit

Website : 8fit.com

Bio : In July 2018, the health and fitness service 8fit suffered a data breach. The data subsequently appeared for sale on a dark web marketplace in February 2019 and included over 15M unique email addresses alongside names, genders, IP addresses and



passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Creation Date : 2018-07-01T00:00:00

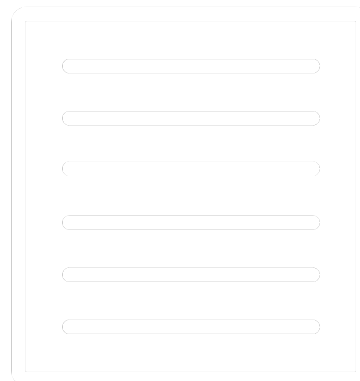
Registered : true

Breach : true

Name : Anti Public Combo List

Bio : In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I Been Pwned](https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned).

Creation Date : 2016-12-16T00:00:00



Registered : true

Breach : true

Name : ClearVoice Surveys

Website : clearvoicesurveys.com

Bio : In April 2021, the market research surveys company ClearVoice Surveys had a publicly facing database backup from 2015 taken and redistributed on a popular hacking forum. The data included 15M unique email addresses across more than 17M rows of data that also included names, physical and IP addresses, genders, dates of birth and plain text passwords. ClearVoice Surveys advised they were aware of the breach and confirmed its authenticity.

Creation Date : 2015-08-23T00:00:00



Registered : true

Breach : true

Name : Evite

Website : evite.com

Bio : In April 2019, the social planning website for managing online invitations 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. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

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

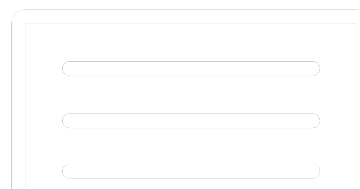


Registered : true

Breach : true

Name : Exploit.In

Bio : In late 2016, a huge list of email address and password



pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I Been Pwned](https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned).

Creation Date : 2016-10-13T00:00:00

Registered : true

Breach : true

Name : Lead Hunter

Bio : In March 2020, [a massive trove of personal information referred to as "Lead Hunter"](https://www.troyhunt.com/the-unattributable-lead-hunter-data-breach) was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. The data contained 69 million unique email addresses across 110 million rows of data accompanied by additional personal information including names, phone numbers, genders and physical addresses. At the time of publishing, the breach could not be attributed to those responsible for obtaining and exposing it. The data was provided to HIBP by dehashed.com.

Creation Date : 2020-03-04T00:00:00

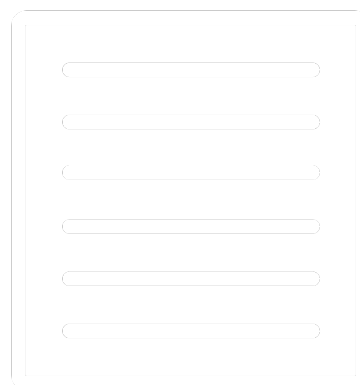
Registered : true

Breach : true

Name : MyFitnessPal

Website : myfitnesspal.com

Bio : In February 2018, the diet and exercise service [A rectangular placeholder box containing three horizontal lines, indicating a missing image or logo.](https://</p></div><div data-bbox=)



content.myfitnesspal.com/security-information/FAQ.html" target="_blank" rel="noopener">MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Creation Date : 2018-02-01T00:00:00

Registered : true

Breach : true

Name : MySpace

Website : myspace.com

Bio : In approximately 2008,

MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

Creation Date : 2008-07-01T00:00:00

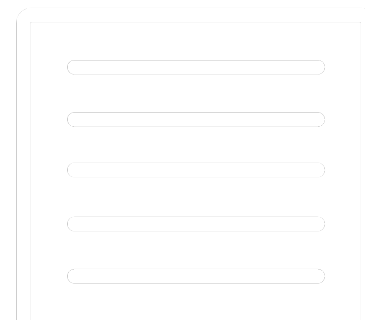


Registered : true

Breach : true

Name : Data Enrichment Exposure From PDL Customer

Bio : 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.

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

Registered : true

Breach : true

Name : Poshmark

Website : poshmark.com

Bio : In mid-2018, social commerce marketplace Poshmark suffered a data breach that exposed 36M user accounts. The compromised data included email addresses, names, usernames, genders, locations and passwords stored as bcrypt hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Creation Date : 2018-05-16T00:00:00

Registered : true

Breach : true

Name : Straffix

Website : straffix.io

Bio : In February 2020, Israeli marketing company Straffix exposed a database with 140GB of personal data. The publicly accessible Elasticsearch database contained over 300M rows with 49M unique email addresses. Exposed data also included names, phone numbers, physical addresses and genders. In <a



href="https://straffic.io/updates.php" target="_blank" rel="noopener">their breach disclosure message, Straffic stated that "it is impossible to create a totally immune system, and these things can occur".

Creation Date : 2020-02-14T00:00:00

Registered : true

Breach : true

Name : Verifications.io

Website : verifications.io

Bio : In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, 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.

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



MYSPACE

Registered : true

SNAPCHAT

Registered : true

TAGGED

Registered : true

CYBERBACKGROUNDCHECKS

Registered : true

Name : Lacoinda Rochell Haggerty

Location : 5300 S Lake Houston Pkwy, Houston, TX, 77049, US

Email : lacoinda@gmail.com, ronald.robinson73@gmail.com, kingscolony7123@yahoo.com, d81857@yahoo.com, lrhaggerty@yahoo.com, mz_bri812@yahoo.com, abrianah@yahoo.com, abrianah2@yahoo.com, sexy_q@hotmail.com, sexy_q1980@hotmail.com, lacoinda.haggerty@yahoo.com

ESPN

Registered : true

PHOTOBUCKET

Registered : true

INSTAGRAM

Registered : true

SAMSUNG

Registered : true

Phone Hint : +128**91**30

BIBLE

Registered : true

Id : 15767480

Name : lacoinda80

Language : English

Username : lacoinda80

Profile Url : <https://my.bible.com/users/15767480>

Creation Date : 2012-09-23T13:03:14.451789+00:00

DISNEY

Registered : true

PINTEREST

Registered : true

EBAY

Registered : true

First Name : LaCoinda

Location : United States

Username : lacoagg-0

Profile Url : <https://www.ebay.com/usr/lacoagg-0>

Phone Hint : 2**-***-**30

Creation Date : 2020-05-28T00:00:00



MICROSOFT

Registered : true

Id : D51136C0F10A52A6

Name : LaCoinda Haggerty

Location : US

Last Seen : 2024-09-01T08:44:35.050000+00:00

Creation Date : 2018-12-23T07:07:50.143000+00:00

MAPS

Registered : true

Profile Url : <https://www.google.com/maps/contrib/108050409165180930563/reviews>

Timeline

Content: Breached on 8fit

Date/Year: 2018-07-01T00:00:00

Content: Breached on Anti Public Combo List

Date/Year: 2016-12-16T00:00:00

Content: Breached on ClearVoice Surveys

Date/Year: 2015-08-23T00:00:00

Content: Breached on Evite

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

Content: Breached on Exploit.In

Date/Year: 2016-10-13T00:00:00

Content: Breached on Lead Hunter

Date/Year: 2020-03-04T00:00:00

Content: Breached on MyFitnessPal

Date/Year: 2018-02-01T00:00:00

Content: Breached on MySpace

Date/Year: 2008-07-01T00:00:00

Content: Breached on Data Enrichment Exposure From PDL Customer

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

Content: Breached on Poshmark

Date/Year: 2018-05-16T00:00:00

Content: Breached on Straffric

Date/Year: 2020-02-14T00:00:00

Content: Breached on Verifications.io

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

Content: Created Account (Bible)

Date/Year: 2012-09-23T13:03:14.451789+00:00

Content: Created Account (Ebay)

Date/Year: 2020-05-28T00:00:00

Content: Last Active (Microsoft)

Date/Year: 2024-09-01T08:44:35.050000+00:00

Content: Created Account (Microsoft)

Date/Year: 2018-12-23T07:07:50.143000+00:00

Content: Last Active (Google)

Date/Year: 2023-03-26T00:14:34

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