Report for: dishxchicago@yahoo.com

As of 2024-07-26T03:27:54.551Z

Minified and concise search report.

Module Responses:

MYSPACE

Registered: true

HIBP

Picture Url

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 &quot;combo list&quot; referred to as &quot;Anti Public&quot;. 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 &quot;credential stuffing&quot;, 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 <a href="https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned" target="_blank" rel="noopener">Password reuse, credential stuffing and another billion records in Have I Been Pwned</a>.
Creation Date: 2016-12-16T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In December 2016, a huge list of email address and password pairs appeared in a &quot;combo list&quot; referred to as &quot;Anti Public&quot;. 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 &quot;credential stuffing&quot;, 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 <a href="https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned" target="_blank" rel="noopener">Password reuse, credential stuffing and another billion records in Have I Been Pwned</a>.
Title: Anti Public Combo List
Breach Count: 457962538

HIBP

Picture Url

Registered: true
Breach: true
Name: ApexSMS
Bio: In May 2019, <a href="https://techcrunch.com/2019/05/09/sms-spammers-doxxed/?guccounter=1" target="_blank" rel="noopener">news broke of a massive SMS spam operation known as &quot;ApexSMS&quot; which was discovered after a MongoDB instance of the same name was found exposed without a password</a>. The incident leaked over 80M records with 23M unique email addresses alongside names, phone numbers and carriers, geographic locations (state and country), genders and IP addresses.
Creation Date: 2019-04-15T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In May 2019, <a href="https://techcrunch.com/2019/05/09/sms-spammers-doxxed/?guccounter=1" target="_blank" rel="noopener">news broke of a massive SMS spam operation known as &quot;ApexSMS&quot; which was discovered after a MongoDB instance of the same name was found exposed without a password</a>. The incident leaked over 80M records with 23M unique email addresses alongside names, phone numbers and carriers, geographic locations (state and country), genders and IP addresses.
Title: ApexSMS
Breach Count: 23246481

HIBP

Picture Url

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</a>. 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
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: 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</a>. 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.

Title: Data Enrichment Exposure From PDL Customer

Breach Count: 622161052

HIBP

Picture Url

Registered: true

Breach: true

Name: Modern Business Solutions

Website: modbsolutions.com

Bio: In October 2016, a large Mongo DB file containing tens of millions of accounts <a href="https://twitter.com/0x2Taylor/status/784544208879292417" target="_blank" rel="noopener">was shared publicly on Twitter</a> (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently <a href="http://news.softpedia.com/news/hacker-steals-58-million-user-records-from-data-storage-provider-509190.shtml" target="_blank" rel="noopener">attributed to &quot;Modern Business Solutions&quot;</a>, a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.

Creation Date: 2016-10-08T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ModernBusinessSolutions.png

Website: modbsolutions.com

Description: In October 2016, a large Mongo DB file containing tens of millions of accounts <a href="https://twitter.com/0x2Taylor/status/784544208879292417" target="_blank" rel="noopener">was shared publicly on Twitter</a> (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently <a href="http://news.softpedia.com/news/hacker-steals-58-million-user-records-from-data-storage-provider-509190.shtml" target="_blank" rel="noopener">attributed to &quot;Modern Business Solutions&quot;</a>, a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.

Title: Modern Business Solutions

Breach Count: 58843488

HIBP

Picture Url

Registered: true

Breach: true

Name: MySpace
Website: myspace.com
Bio: In approximately 2008, <a href="http://motherboard.vice.com/read/427-million-myspace-passwords-emails-data-breach" target="_blank" rel="noopener">MySpace suffered a data breach that exposed almost 360 million accounts</a>. In May 2016 the data was offered up for sale on the &quot;Real Deal&quot; 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 <a href="https://www.troyhunt.com/dating-the-ginormous-myspace-breach" target="_blank" rel="noopener">analysis of the data suggests it was 8 years before being made public</a>.
Creation Date: 2008-07-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/MySpace.png
Website: myspace.com
Description: In approximately 2008, <a href="http://motherboard.vice.com/read/427-million-myspace-passwords-emails-data-breach" target="_blank" rel="noopener">MySpace suffered a data breach that exposed almost 360 million accounts</a>. In May 2016 the data was offered up for sale on the &quot;Real Deal&quot; 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 <a href="https://www.troyhunt.com/dating-the-ginormous-myspace-breach" target="_blank" rel="noopener">analysis of the data suggests it was 8 years before being made public</a>.
Title: MySpace
Breach Count: 359420698

HIBP

Picture Url

Registered: true
Breach: true
Name: Verifications.io
Website: verifications.io
Bio: In February 2019, the email address validation service <a href="https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service" target="_blank" rel="noopener">verifications.io suffered a data breach</a>. Discovered by <a href="https://twitter.com/mayhemdayone" target="_blank" rel="noopener">Bob Diachenko</a> and <a href="https://twitter.com/vinnytroia" target="_blank" rel="noopener">Vinny Troia</a>, 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 <a href="https://web.archive.org/web/20190227230352/https://verifications.io/" target="_blank" rel="noopener">an archived copy remains viewable</a>.
Creation Date: 2019-02-25T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/VerificationsIO.png
Website: verifications.io
Description: In February 2019, the email address validation service <a href="https://

securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service" target="_blank" rel="noopener">verifications.io suffered a data breach</a>. Discovered by <a href="https://twitter.com/mayhemdayone" target="_blank" rel="noopener">Bob Diachenko</a> and <a href="https://twitter.com/vinnytroia" target="_blank" rel="noopener">Vinny Troia</a>, 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 <a href="https://web.archive.org/web/20190227230352/https://verifications.io/" target="_blank" rel="noopener">an archived copy remains viewable</a>.

Title: Verifications.io

Breach Count: 763117241

PANDORA

Picture Url
Profile Url

Registered: true
Username: dishxchicago
Followers: 0
Following: 0
Likes: 0
Stations: 2

EA

Registered: true

MAPS

Profile Url

Registered: true

GOOGLE

Picture Url

Registered: true
Id: 102682750088629417136
Last Seen: 2023-08-23T12:41:31