Report for: chris.elder@gmail.com

As of 2025-07-26T07:14:17.273Z

Minified and concise search report.

Module Responses:

HIBP

Picture Url

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 adding further to the risk that hundreds of millions of Adobe customers already faced.
Creation Date: 2013-10-04T00:00:00
Logo: https://logos.haveibeenpwned.com/Adobe.png
Website: adobe.com
Description: 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 adding further to the risk that hundreds of millions of Adobe customers already faced.
Title: Adobe
Modified Date: 2022-05-15T23:52:49Z
Breach Count: 152445165

HIBP

Picture Url

Registered: true
Breach: true
Name: Stratfor
Website: stratfor.com
Bio: In December 2011, "Anonymous" <a href="http://www.troyhunt.com/2011/12/5-

website-security-lessons-courtesy-of.html" target="_blank" rel="noopener">attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Creation Date: 2011-12-24T00:00:00

Logo: https://logos.haveibeenpwned.com/Stratfor.png

Website: stratfor.com

Description: In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Title: Stratfor

Modified Date: 2013-12-04T00:00:00Z

Breach Count: 859777

HIBP

Picture Url

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

Logo: https://logos.haveibeenpwned.com/MySpace.png

Website: myspace.com

Description: 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.

Title: MySpace
Modified Date: 2016-05-31T00:12:29Z
Breach Count: 359420698

HIBP

Picture Url

Registered: true
Breach: true
Name: Dropbox
Website: dropbox.com
Bio: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
Creation Date: 2012-07-01T00:00:00
Logo: https://logos.haveibeenpwned.com/Dropbox.png
Website: dropbox.com
Description: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
Title: Dropbox
Modified Date: 2016-08-31T00:19:19Z
Breach Count: 68648009

HIBP

Picture Url

Registered: true
Breach: true
Name: River City Media Spam List
Website: rivercitymediaonline.com
Bio: In January 2017, <a href="https://web.archive.org/web/20170426084052/https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire" target="_blank"

rel="noopener">a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Creation Date: 2017-01-01T00:00:00

Logo: https://logos.haveibeenpwned.com/Email.png

Website: rivercitymediaonline.com

Description: In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Title: River City Media Spam List

Modified Date: 2017-03-08T23:49:53Z

Breach Count: 393430309

HIBP

Picture Url

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.

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

Logo: https://logos.haveibeenpwned.com/List.png

Description: 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.

Title: Exploit.In

Modified Date: 2017-05-06T07:03:18Z

Breach Count: 593427119

HIBP

Picture Url

Registered: true
Breach: true
Name: Kickstarter
Website: kickstarter.com
Bio: In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.
Creation Date: 2014-02-16T00:00:00
Logo: https://logos.haveibeenpwned.com/Kickstarter.png
Website: kickstarter.com
Description: In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.
Title: Kickstarter
Modified Date: 2017-10-06T07:29:07Z
Breach Count: 5176463

HIBP

Picture Url

Registered: true
Breach: true
Name: Kayo.moe Credential Stuffing List
Bio: In September 2018, a collection of almost 42 million email address and plain text password pairs was uploaded to the anonymous file sharing service kayo.moe. The operator of the service contacted HIBP to report the data which, upon further investigation, turned out to be a large credential stuffing list. For more information, read about The 42M Record kayo.moe Credential Stuffing Data.
Creation Date: 2018-09-11T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In September 2018, a collection of almost 42 million email address and plain text password pairs was uploaded to the anonymous file sharing service kayo.moe. The operator of the service contacted HIBP to report the data which, upon further investigation, turned out to be a large credential stuffing list. For more information, read about The 42M Record kayo.moe Credential Stuffing Data.

Title: Kayo.moe Credential Stuffing List
Modified Date: 2018-09-13T20:12:18Z
Breach Count: 41826763

HIBP

Picture Url

Registered: true
Breach: true
Name: Collection #1
Bio: In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.
Creation Date: 2019-01-07T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.
Title: Collection #1
Modified Date: 2019-01-16T21:50:21Z
Breach Count: 772904991

HIBP

Picture Url

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

Logo: https://logos.haveibeenpwned.com/VerificationsIO.png

Website: verifications.io

Description: 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.

Title: Verifications.io

Modified Date: 2019-03-09T20:49:51Z

Breach Count: 763117241

HIBP

Picture Url

Registered: true

Breach: true

Name: Gravatar

Website: gravatar.com

Bio: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Creation Date: 2020-10-03T00:00:00

Logo: https://logos.haveibeenpwned.com/Gravatar.png

Website: gravatar.com

Description: In October 2020, <a href="https://www.bleepingcomputer.com/news/security/online-avatar-service-gravatar-allows-mass-collection-of-user-info/" target="_blank"

rel="noopener">a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.
Title: Gravatar
Modified Date: 2021-12-08T01:47:02Z
Breach Count: 113990759

HIBP

Picture Url

Registered: true
Breach: true
Name: Naz.API
Bio: In September 2023, over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.
Creation Date: 2023-09-20T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In September 2023, over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.
Title: Naz.API
Modified Date: 2024-01-17T13:24:27Z
Breach Count: 70840771

HIBP

Picture Url

Registered: true
Breach: true
Name: Combolists Posted to Telegram
Bio: In May 2024, 2B rows of data with 361M unique email addresses

were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.

Creation Date: 2024-05-28T00:00:00

Logo: https://logos.haveibeenpwned.com/List.png

Description: In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.

Title: Combolists Posted to Telegram

Modified Date: 2024-06-11T07:01:09Z

Breach Count: 361468099

HIBP

Picture Url

Registered: true

Breach: true

Name: Not SOCRadar

Bio: In August 2024, over 332M rows of email addresses were posted to a popular hacking forum. The post alleged the addresses were scraped from cybersecurity firm SOCRadar, however an investigation on their behalf concluded that "the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources". There is no suggestion the incident compromised SOCRadar's security or posed any risk to their customers. In total, the data set contained 282M unique addresses of valid email address format.

Creation Date: 2024-08-03T00:00:00

Logo: https://logos.haveibeenpwned.com/List.png

Description: In August 2024, over 332M rows of email addresses were posted to a popular hacking forum. The post alleged the addresses were scraped from cybersecurity firm SOCRadar, however an investigation on their behalf concluded that "the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources". There is no suggestion the incident compromised SOCRadar's security or posed any risk to their customers. In total, the data set contained 282M unique addresses of valid email address format.

Title: Not SOCRadar

Modified Date: 2024-08-09T09:28:24Z

Breach Count: 282478425

HIBP

Picture Url

Registered: true
Breach: true
Name: French Citizens
Bio: In September 2024, over 90M rows of data on French Citizens was found left exposed in a publicly facing database. Compiled from various data breaches, the corpus contained 28M unique email addresses with the various source breaches each exposing different fields including name, physical and IP address, phone number and partial credit card data including payment type and last 4 digits.
Creation Date: 2024-09-25T00:00:00
Logo: https://logos.haveibeenpwned.com/France.png
Description: In September 2024, over 90M rows of data on French Citizens was found left exposed in a publicly facing database. Compiled from various data breaches, the corpus contained 28M unique email addresses with the various source breaches each exposing different fields including name, physical and IP address, phone number and partial credit card data including payment type and last 4 digits.
Title: French Citizens
Modified Date: 2024-12-20T09:54:50Z
Breach Count: 28445106

HIBP

Picture Url

Registered: true
Breach: true
Name: ALIEN TXTBASE Stealer Logs
Bio: In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.
Creation Date: 2025-02-15T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.
Title: ALIEN TXTBASE Stealer Logs
Modified Date: 2025-02-25T19:25:18Z
Breach Count: 284132969

NEWYORKTIMES

Registered: true
Id: 135646062

VIMEO

Registered: true

DISNEY

Registered: true

FOURSQUARE

Picture Url
Profile Url

Registered: true
Id: 130908
Name: Chris Elder
First Name: Chris
Last Name: Elder
Gender: Male
Location: NZ
Username: chrise1133592
Private: false
Home City: Wellington, New Zealand

PINTEREST

Registered: true

GRAVATAR

Picture Url
Profile Url

Registered: true
Id: dc0322dc7b59eb32169f53727173195abe6fc7211615678b020d91832134da5c
Name: one3nine
Username: one3nine

TRELLO

Profile Url

Registered: true
Id: 4e7020d48e611c0000018f9c
Name: Chris Elder
Username: chriselder
Last Seen: 2012-07-04T07:53:17.945000+00:00
Member Type: normal

4SHARED

Registered: true

ESPN

Registered: true

WORDPRESS

Registered: true

FLICKR

Picture Url
Profile Url

Registered: true
Id: 85929084@N03
Name: Chris Elder
Username: Chris Elder
Followers: 2
Creation Date: 2012-08-27T15:05:33

MYSPACE

Picture Url
Profile Url

Registered: true
Id: onethreenine
Name: Chris Elder
Username: onethreenine
Followers: 0
Following: 0

MYSPACE

Picture Url
Profile Url

Registered: true
Id: chrisellej67.gmail.com
Name: Chriselle Jimenez
Username: chrisellej67.gmail.com
Followers: 2
Following: 0

FITBIT

Picture Url

Registered: true
Id: 3744SS

Name: Chris E.
Type: person

EVENTBRITE

Registered: true
Id: 3488171468
Verified: false

MAPS

Profile Url

Registered: true

GOOGLE

Picture Url

Registered: true
Id: 105262943336415667297
Last Seen: 2023-10-27T02:05:28

DROPBOX

Registered: true
Id: dbid:AABSllJ8qRxvJLP0lbfFmsziJASl07rughw
Name: Chris Elder
First Name: Chris
Last Name: Elder
Verified: true
