Report for: stephaniemartin@gmail.com

As of 2024-09-16T20:42:16.884Z

Minified and concise search report.

Module Responses:

SPOTIFY

Registered: true

REDFIN

Registered: true

TWITTER

Registered: true

ADOBE

Registered: true
Status: active
Type: individual

ZILLOW

Registered: true

MYSPACE

Registered: true

TUMBLR

Registered: true

INSTAGRAM

Registered: true

POSHMARK

Picture Url
Profile Url

Registered: true
Id: 5abd7af372d0f04078c8ac82
Name: Stephanie Martin
Gender: female
Location: us
Username: stephaniemar226
Creation Date: 2018-03-29T23:46:59
Display Handle: stephaniemar226
Facebook Id: 431332017295792
Status: active
City: Rockwood
State: PA
Registration Method: fb
Registration App: android

FOURSQUARE

Picture Url
Profile Url

Registered: true
Id: 70928646
First Name: Steph
Last Name: Martin
Gender: female
Location: CA
Username: stephm4848089
Private: false
Home City: Coaldale, AB

PICSART

Picture Url
Profile Url

Registered: true
Id: 384395447016101
Username: stephaniemartin4227
Followers: 0
Following: 1
Likes Count: 1
Photos Count: 0
Stickers Public Count: 0

KHANACADEMY

Picture Url
Profile Url

Registered: true
Id: kaid_401866056070578859528432
Name: Estefany Martin
Username: Estefany Martin
Points: 0

SNAPCHAT

Registered: true

SAMSUNG

Registered: true

FITBIT

Profile Url

Registered: true
Id: 6MVP69
Name: Stephanie M.
Type: person

KAHOOT

Registered: true

ESPN

Registered: true

TOYOTA

Registered: true

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: 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 <em>billion</em> 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 <a href="https://www.troyhunt.com/the-773-million-record-collection-1-data-reach" target="_blank" rel="noopener">The 773 Million Record "Collection #1" Data Breach</a>.

Creation Date: 2019-01-07T00:00:00

Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/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 <em>billion</em> 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 <a href="https://www.troyhunt.com/the-773-million-record-collection-1-data-reach" target="_blank" rel="noopener">The 773 Million Record "Collection #1" Data Breach</a>.

Title: Collection #1

Breach Count: 772904991

HIBP

Picture Url

Registered: true

Breach: true

Name: Deezer

Website: deezer.com

Bio: In late 2022, the music streaming service <a href="https://restoreprivacy.com/music-service-deezer-data-breach/" target="_blank" rel="noopener">Deezer disclosed a data breach that impacted over 240M customers</a>. The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.

Creation Date: 2019-04-22T00:00:00

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

Website: deezer.com

Description: In late 2022, the music streaming service <a href="https://restoreprivacy.com/music-service-deezer-data-breach/" target="_blank" rel="noopener">Deezer disclosed a data breach that impacted over 240M customers</a>. The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.

Title: Deezer

Breach Count: 229037936

HIBP

Picture Url

Registered: true

Breach: true

Name: DriveSure

Website: drivesure.com

Bio: In December 2020, the car dealership service provider <a href="https://www.riskbasedsecurity.com/2021/02/01/personal-data-of-3-million-people-exposed-in-drivesure-hack/" target="_blank" rel="noopener">DriveSure suffered a data breach</a>. The incident resulted in 26GB of data being downloaded and later shared on a hacking forum. Impacted personal information included 3.6 million unique email addresses, names, phone numbers and physical addresses. Vehicle data was also exposed and included makes, models, VIN numbers and odometer readings. A small number of passwords stored as bcrypt hashes were also included in the data set.

Creation Date: 2020-12-19T00:00:00

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

Website: drivesure.com

Description: In December 2020, the car dealership service provider <a href="https://www.riskbasedsecurity.com/2021/02/01/personal-data-of-3-million-people-exposed-in-drivesure-hack/" target="_blank" rel="noopener">DriveSure suffered a data breach</a>. The incident resulted in 26GB of data being downloaded and later shared on a hacking forum. Impacted personal information included 3.6 million unique email addresses, names, phone numbers and physical addresses. Vehicle data was also exposed and included makes, models, VIN numbers and odometer readings. A small number of passwords stored as bcrypt hashes

were also included in the data set.
Title: DriveSure
Breach Count: 3675099

HIBP

Picture Url

Registered: true
Breach: true
Name: Dubsmash
Website: dubsmash.com
Bio: In December 2018, the video messaging service <a href="https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/" target="_blank" rel="noopener">Dubsmash suffered a data breach</a>. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. 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 &quot;BenjaminBlue@exploit.im&quot;.
Creation Date: 2018-12-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Dubsmash.png
Website: dubsmash.com
Description: In December 2018, the video messaging service <a href="https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/" target="_blank" rel="noopener">Dubsmash suffered a data breach</a>. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. 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 &quot;BenjaminBlue@exploit.im&quot;.
Title: Dubsmash
Breach Count: 161749950

HIBP

Picture Url

Registered: true
Breach: true
Name: Duolingo
Website: duolingo.com
Bio: In August 2023, <a href="https://www.bleepingcomputer.com/news/security/scraped-data-of-26-million-duolingo-users-released-on-hacking-forum/" target="_blank" rel="noopener">2.6M records of data scraped from Duolingo were broadly distributed on a popular hacking forum</a>. Obtained by enumerating a vulnerable API, the data had earlier appeared for sale in January 2023 and contained email addresses, names, the languages being learned, XP (experience points), and other data related to learning progress on Duolingo. Whilst some of the data attributes are

intentionally public, the ability to map private email addresses to them presents an ongoing risk to user privacy.

Creation Date: 2023-01-24T00:00:00

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

Website: duolingo.com

Description: In August 2023, <a href="https://www.bleepingcomputer.com/news/security/scraped-data-of-26-million-duolingo-users-released-on-hacking-forum/" target="_blank" rel="noopener">2.6M records of data scraped from Duolingo were broadly distributed on a popular hacking forum</a>. Obtained by enumerating a vulnerable API, the data had earlier appeared for sale in January 2023 and contained email addresses, names, the languages being learned, XP (experience points), and other data related to learning progress on Duolingo. Whilst some of the data attributes are intentionally public, the ability to map private email addresses to them presents an ongoing risk to user privacy.

Title: Duolingo

Breach Count: 2676696

HIBP

Picture Url

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&lctid=1800182" target="_blank" rel="noopener">Evite identified a data breach of their systems</a>. 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 &quot;JimScott.Sec@protonmail.com&quot;.

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

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

Website: evite.com

Description: In April 2019, the social planning website for managing online invitations <a href="https://www.evite.com/security/update?usource=lc&lctid=1800182" target="_blank" rel="noopener">Evite identified a data breach of their systems</a>. 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 &quot;JimScott.Sec@protonmail.com&quot;.

Title: Evite

Breach Count: 100985047

HIBP

Picture Url

Registered: true
Breach: true
Name: Lead Hunter
Bio: In March 2020, <a href="https://www.troyhunt.com/the-unattributable-lead-hunter-data-breach" target="_blank" rel="noopener">a massive trove of personal information referred to as &quot;Lead Hunter&quot;</a> 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 <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.
Creation Date: 2020-03-04T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In March 2020, <a href="https://www.troyhunt.com/the-unattributable-lead-hunter-data-breach" target="_blank" rel="noopener">a massive trove of personal information referred to as &quot;Lead Hunter&quot;</a> 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 <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.
Title: Lead Hunter
Breach Count: 68693853

HIBP

Picture Url

Registered: true
Breach: true
Name: LinkedIn
Website: linkedin.com
Bio: In May 2016, <a href="https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach" target="_blank" rel="noopener">LinkedIn had 164 million email addresses and passwords exposed</a>. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.
Creation Date: 2012-05-05T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/LinkedIn.png
Website: linkedin.com
Description: In May 2016, <a href="https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach" target="_blank" rel="noopener">LinkedIn had 164 million email addresses and passwords exposed</a>. Originally hacked in 2012, the data remained out of sight until

being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Title: LinkedIn

Breach Count: 164611595

HIBP

Picture Url

Registered: true

Breach: true

Name: Mathway

Website: mathway.com

Bio: In January 2020, the math solving website <a href="https://www.zdnet.com/article/25-million-user-records-leak-online-from-popular-math-app-mathway/" target="_blank" rel="noopener">Mathway suffered a data breach that exposed over 25M records</a>. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.

Creation Date: 2020-01-13T00:00:00

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

Website: mathway.com

Description: In January 2020, the math solving website <a href="https://www.zdnet.com/article/25-million-user-records-leak-online-from-popular-math-app-mathway/" target="_blank" rel="noopener">Mathway suffered a data breach that exposed over 25M records</a>. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.

Title: Mathway

Breach Count: 25692862

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: National Public Data

Bio: In April 2024, <a href="https://www.troyhunt.com/inside-the-3-billion-people-national-public-data-breach" target="_blank" rel="noopener">a large trove of data made headlines as having exposed &quot;3 billion people&quot; due to a breach of the National Public Data background check service</a>. The initial corpus of data released in the breach contained billions of rows of personal information, including US social security numbers. Further partial data sets were later released including extensive personal information and 134M unique email addresses, although the origin and accuracy of the data remains in question. This breach has been flagged as &quot;unverified&quot; and a full description of the incident is in the link above.

Creation Date: 2024-04-09T00:00:00

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

Description: In April 2024, <a href="https://www.troyhunt.com/inside-the-3-billion-people-national-public-data-breach" target="_blank" rel="noopener">a large trove of data made headlines as having exposed &quot;3 billion people&quot; due to a breach of the National Public Data background check service</a>. The initial corpus of data released in the breach contained billions of rows of personal information, including US social security numbers. Further partial data sets were later released including extensive personal information and 134M unique email addresses, although the origin and accuracy of the data remains in question. This breach has been flagged as &quot;unverified&quot; and a full description of the incident is in the link above.

Title: National Public Data

Breach Count: 133957569

HIBP

Picture Url

Registered: true
Breach: true
Name: Neiman Marcus
Website: neimanmarcus.com
Bio: In May 2024, the American luxury retailer Neiman Marcus suffered a data breach <a href="https://www.bleepingcomputer.com/news/security/neiman-marcus-data-breach-31-million-email-addresses-found-exposed/" target="_blank" rel="noopener">which was later posted to a popular hacking forum</a>. The data included 31M unique email addresses, names, phone numbers, dates of birth, physical addresses and partial credit card data (note: this is insufficient to make purchases). The breach was traced back to a series of attacks against the Snowflake cloud service which impacted 165 organisations worldwide.
Creation Date: 2024-04-14T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/NeimanMarcus.png
Website: neimanmarcus.com
Description: In May 2024, the American luxury retailer Neiman Marcus suffered a data breach <a href="https://www.bleepingcomputer.com/news/security/neiman-marcus-data-breach-31-million-email-addresses-found-exposed/" target="_blank" rel="noopener">which was later posted to a popular hacking forum</a>. The data included 31M unique email addresses, names, phone numbers, dates of birth, physical addresses and partial credit card data (note: this is insufficient to make purchases). The breach was traced back to a series of attacks against the Snowflake cloud service which impacted 165 organisations worldwide.
Title: Neiman Marcus
Breach Count: 31152842

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: Poshmark
Website: poshmark.com
Bio: In mid-2018, social commerce marketplace <a href="https://techcrunch.com/2019/08/01/poshmark-confirms-data-breach/" target="_blank" rel="noopener">Poshmark suffered a data breach</a> 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
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Poshmark.png
Website: poshmark.com
Description: In mid-2018, social commerce marketplace <a href="https://techcrunch.com/2019/08/01/poshmark-confirms-data-breach/" target="_blank" rel="noopener">Poshmark suffered a data breach</a> 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".
Title: Poshmark
Breach Count: 36395491

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</a>. 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://haveibeenpwned.com/Content/Images/PwnedLogos/Email.png

Website: rivercitymediaonline.com
Description: 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</a>. 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
Breach Count: 393430309

HIBP

Picture Url

Registered: true
Breach: true
Name: Combolists Posted to Telegram
Bio: In May 2024, <a href="https://troyhunt.com/telegram-combolists-and-361m-email-addresses" target="_blank" rel="noopener">2B rows of data with 361M unique email addresses were collated from malicious Telegram channels</a>. 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://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In May 2024, <a href="https://troyhunt.com/telegram-combolists-and-361m-email-addresses" target="_blank" rel="noopener">2B rows of data with 361M unique email addresses were collated from malicious Telegram channels</a>. 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
Breach Count: 361468099

HIBP

Picture Url

Registered: true
Breach: true
Name: Twitter (200M)
Website: twitter.com
Bio: In early 2023, <a href="https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/" target="_blank" rel="noopener">over 200M records scraped from Twitter appeared on a popular hacking forum</a>. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to

Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.

Creation Date: 2021-01-01T00:00:00

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

Website: twitter.com

Description: In early 2023, <a href="https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/" target="_blank" rel="noopener">over 200M records scraped from Twitter appeared on a popular hacking forum</a>. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.

Title: Twitter (200M)

Breach Count: 211524284

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

HIBP

Picture Url

Registered: true

Breach: true

Name: Wakanim

Website: wakanim.tv

Bio: In August 2022, the European streaming service <a href="https://www.animenewsnetwork.com/news/2022-09-07/wakanim-streaming-service-delays-content-after-possible-data-breach/.189234" target="_blank" rel="noopener">Wakanim suffered a data breach which was subsequently advertised and sold on a popular hacking forum</a>. The breach exposed 6.7M customer records including email, IP and physical addresses, names and usernames.

Creation Date: 2022-08-28T00:00:00

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

Website: wakanim.tv

Description: In August 2022, the European streaming service <a href="https://www.animenewsnetwork.com/news/2022-09-07/wakanim-streaming-service-delays-content-after-possible-data-breach/.189234" target="_blank" rel="noopener">Wakanim suffered a data breach which was subsequently advertised and sold on a popular hacking forum</a>. The breach exposed 6.7M customer records including email, IP and physical addresses, names and usernames.

Title: Wakanim

Breach Count: 6706951

HIBP

Picture Url

Registered: true

Breach: true

Name: Zynga

Website: zynga.com

Bio: In September 2019, game developer <a href="https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/" target="_blank" rel="noopener">Zynga (the creator of Words with Friends) suffered a data breach</a>. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.

Creation Date: 2019-09-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Zynga.png
Website: zynga.com
Description: In September 2019, game developer <a href="https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/" target="_blank" rel="noopener">Zynga (the creator of Words with Friends) suffered a data breach</a>. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by <a href="https://dehashed.com/" target="_blank" rel="noopener">dehashed.com</a>.
Title: Zynga
Breach Count: 172869660

DISNEY

Registered: true

SMULE

Profile Url

Registered: true
Id: 1516246796
Username: Stephanie100732
Verified: false
Jid: 1516246796@j.smule.com
Picture Type: default

PANDORA

Picture Url
Profile Url

Registered: true
Username: stephaniemartin08
Followers: 0
Following: 0
Likes: 2
Stations: 1

MICROSOFT

Registered: true

WORDPRESS

Registered: true

EA

Registered: true

LINKEDIN

Registered: true

GAANA

Registered: true

PINTEREST

Registered: true

ECONOMICTIMES

Registered: true

RUMBLE

Profile Url

Registered: true
Id: _u2w8dne
Name: hrtgodtgzqfuewmooehv
Username: hrtgodtgzqfuewmooehv
Followers: 0
Following: 0
Verified: false
Creation Date: 2023-09-27T00:00:00
Type: user
Videos: 0
Rumbles: 0

MAPS

Profile Url

Registered: true

GOOGLE

Picture Url

Registered: true
Id: 108593316854633131309
Last Seen: 2023-03-21T09:14:29

AIRBNB

Picture Url

Registered: true
First Name: Stephanie

DUOLINGO

Picture Url

Profile Url

Registered: true
Id: 222663745
Name: stephanie martin
Username: stephaniem271554
Premium: false
Creation Date: 2016-10-11T16:43:44
Learning Language: en
From Language: fr
Motivation: none
Total Xp: 100
Streak: 0
Current Course Id: DUOLINGO_EN_FR

PAYPAL

Registered: true
Phone Hint: +1 6**-***-3762
Acc Number: 1702********4945
