Report for: stephaniemartin5412@gmail.com

As of 2024-09-16T18:18:31.118Z

Minified and concise search report.

Module Responses:

TALENT

Registered: true

REMIND

Registered: true

REPLIT

Registered: true

INSTACART

Registered: true

TRIVAGO

Registered: true

ADOBE

Registered: true
Status: active
Type: individual

SNAPCHAT

Registered: true

SPOTIFY

Registered: true

VIMEO

Registered: true

ETSY

[Picture Url]()

Registered: true
Name: stephanie

CASHAPP

[Picture Url]()

Registered: true
Id: C_sep9r0yf3
Name: stephanie martin
Location: USA
Username: steph5412
Verified: false

SAMSUNG

Registered: true
Phone Hint: +120**45**96

KAHOOT

Registered: true

HIBP

Picture Url

Registered: true
Breach: true
Name: Advance Auto Parts
Website: advanceautoparts.com
Bio: In June 2024, <a href="https://www.bleepingcomputer.com/news/security/advance-auto-parts-confirms-data-breach-exposed-employee-information/" target="_blank" rel="noopener">Advance Auto Parts confirmed they had suffered a data breach</a> which was posted for sale to a popular hacking forum. Linked to unauthorised access to Snowflake cloud services, the breach exposed a large number of records related to both customers and employees. In total, 79M unique email addresses were included in the breach, alongside names, phone numbers, addresses and further data attributes related to company employees.
Creation Date: 2024-06-05T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/AdvanceAutoParts.png
Website: advanceautoparts.com
Description: In June 2024, <a href="https://www.bleepingcomputer.com/news/security/advance-auto-parts-confirms-data-breach-exposed-employee-information/" target="_blank" rel="noopener">Advance Auto Parts confirmed they had suffered a data breach</a> which was posted for sale to a popular hacking forum. Linked to unauthorised access to Snowflake cloud services, the breach exposed a large number of records related to both customers and employees. In total, 79M unique email addresses were included in the breach, alongside names, phone numbers, addresses and further data attributes related to company employees.
Title: Advance Auto Parts
Breach Count: 79243727

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: MMG Fusion
Website: mmgfusion.com
Bio: In December 2020, the dental practice management service <a href="https://www.riskbasedsecurity.com/2021/02/19/dark-web-roundup-january-2021/" target="_blank" rel="noopener">MMG Fusion was the victim of a data breach</a> which exposed 2.6M unique email addresses. The data also included patient appointments, names, phone numbers, dates of birth, genders and physical addresses. A small number of records also included passwords stored as bcrypt hashes.
Creation Date: 2020-12-20T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/MMGFusion.png
Website: mmgfusion.com
Description: In December 2020, the dental practice management service <a href="https://www.riskbasedsecurity.com/2021/02/19/dark-web-roundup-january-2021/" target="_blank" rel="noopener">MMG Fusion was the victim of a data breach</a> which exposed 2.6M unique email addresses. The data also included patient appointments, names, phone numbers, dates of birth, genders and physical addresses. A small number of records also included passwords stored as bcrypt hashes.
Title: MMG Fusion
Breach Count: 2660295

HIBP

Picture Url

Registered: true
Breach: true
Name: Not Acxiom
Bio: In 2020, <a href="https://www.troyhunt.com/data-breach-misattribution-acxiom-live-ramp/" target="_blank" rel="noopener">a corpus of data containing almost a quarter of a billion records spanning over 400 different fields was misattributed to database marketing company Acxiom</a> and subsequently circulated within the hacking community. On review, Acxiom concluded that &quot;the claims are indeed false and that the data, which has been readily available across multiple environments, does not come from Acxiom and is in no way the subject of an Acxiom breach&quot;. The data contained almost 52M unique email addresses.
Creation Date: 2020-06-21T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In 2020, <a href="https://www.troyhunt.com/data-breach-misattribution-acxiom-live-ramp/" target="_blank" rel="noopener">a corpus of data containing almost a quarter of a billion records spanning over 400 different fields was misattributed to database marketing company Acxiom</a> and subsequently circulated within the hacking community. On review, Acxiom concluded that &quot;the claims are indeed false and that the data, which has been readily available across multiple environments, does not come from Acxiom and is in no way the subject of an Acxiom breach&quot;. The data contained almost 52M unique email addresses.
Title: Not Acxiom
Breach Count: 51730831

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 <a href="https://socradar.io/socradars-response-to-the-usdods-claim-of-scraping-330-million-emails/" target="_blank" rel="noopener">an investigation on their behalf concluded that &quot;the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources&quot;</a>. 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://haveibeenpwned.com/Content/Images/PwnedLogos/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 <a href="https://socradar.io/socradars-response-to-the-usdods-claim-of-scraping-330-million-emails/" target="_blank" rel="noopener">an investigation on their behalf concluded that

&quot;the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources&quot;</a>. 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

Breach Count: 282478425

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: Special K Data Feed Spam List
Website: data4marketers.com
Bio: In mid to late 2015, a spam list known as the <a href="http://www.data4marketers.com/d4m_SpecialKfeed2015.html" target="_blank" rel="noopener">Special K Data Feed</a> was discovered containing almost 31M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. <a href="https://www.troyhunt.com/have-i-been-pwned-and-spam-lists-of-personal-information" target="_blank" rel="noopener">Read more about spam lists in HIBP.</a>
Creation Date: 2015-10-07T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Email.png
Website: data4marketers.com
Description: In mid to late 2015, a spam list known as the <a href="http://www.data4marketers.com/d4m_SpecialKfeed2015.html" target="_blank" rel="noopener">Special K Data Feed</a> was discovered containing almost 31M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. <a href="https://www.troyhunt.com/have-i-been-pwned-and-spam-lists-of-personal-information" target="_blank" rel="noopener">Read more about spam lists in HIBP.</a>
Title: Special K Data Feed Spam List
Breach Count: 30741620

HIBP

Picture Url

Registered: true
Breach: true
Name: Straffic
Website: straffic.io
Bio: In February 2020, Israeli marketing company <a href="https://www.databreachtoday.com/israeli-marketing-company-exposes-contacts-database-a-13785" target="_blank" rel="noopener">Straffic exposed a database with 140GB of personal data</a>. 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</a>, Straffic stated that &quot;it is impossible to create a totally immune system, and these things can occur&quot;.
Creation Date: 2020-02-14T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Straffic.png
Website: straffic.io
Description: In February 2020, Israeli marketing company <a href="https://www.databreachtoday.com/israeli-marketing-company-exposes-contacts-database-a-13785" target="_blank" rel="noopener">Straffic exposed a database with 140GB of personal data</a>. 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</a>, Straffic stated that &quot;it is impossible to create a totally immune system, and these things can occur&quot;.

Title: Straffic
Breach Count: 48580249

HIBP

[Picture Url]()

Registered: true
Breach: true
Name: The Post Millennial
Website: thepostmillennial.com
Bio: In May 2024, <a href="https://www.mediaite.com/politics/conservative-news-websites-hacked-replaced-with-page-leaking-private-information/" target="_blank" rel="noopener">the conservative news website The Post Millennial suffered a data breach</a>. The breach resulted in the defacement of the website and links posted to 3 different corpuses of data including hundreds of writers and editors (IP, physical address and email exposed), tens of thousands of subscribers to the site (name, email, username, phone and plain text password exposed), and tens of millions of email addresses from <a href="https://sprunge.us/SZTt4N" target="_blank" rel="noopener">thousands of mailing lists</a> <em>alleged</em> to have been used by The Post Millennial (this has not been independently verified). The mailing lists appear to be sourced from various campaigns not necessarily run by The Post Millennial and contain a variety of different personal attributes including name, phone and physical address (depending on the campaign). The data was subsequently posted to a popular hacking forum and extensively torrented.
Creation Date: 2024-05-02T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/ThePostMillennial.png
Website: thepostmillennial.com
Description: In May 2024, <a href="https://www.mediaite.com/politics/conservative-news-websites-hacked-replaced-with-page-leaking-private-information/" target="_blank" rel="noopener">the conservative news website The Post Millennial suffered a data breach</a>. The breach resulted in the defacement of the website and links posted to 3 different corpuses of data including hundreds of writers and editors (IP, physical address and email exposed), tens of thousands of subscribers to the site (name, email, username, phone and plain text password exposed), and tens of millions of email addresses from <a href="https://sprunge.us/SZTt4N" target="_blank" rel="noopener">thousands of mailing lists</a> <em>alleged</em> to have been used by The Post Millennial (this has not been independently verified). The mailing lists appear to be sourced from various campaigns not necessarily run by The Post Millennial and contain a variety of different personal attributes including name, phone and physical address (depending on the campaign). The data was subsequently posted to a popular hacking forum and extensively torrented.
Title: The Post Millennial
Breach Count: 56973345

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

DISNEY

Registered: true

ESPN

Registered: true

FACEBOOK

Registered: true
Email Hint: s*****2@yahoo.com
Phone Hint: +*********96

INSTAGRAM

Registered: true

SKYPE

Picture Url

Registered: true
Id: live:.cid.e53d1a1a77fa3a54
Name: Elijah Martin
Username: live:.cid.e53d1a1a77fa3a54
Contact Type: Skype4Consumer

PANDORA

Picture Url
Profile Url

Registered: true
Username: stephaniemartin5412
Followers: 0
Following: 0
Likes: 397
Stations: 65

ZILLOW

Registered: true

CALLOFDUTY

Registered: true

ACTIVISION

Registered: true

PLAYGAMES

Picture Url
Banner Url

Registered: true
Id: g14134886954459277731
Name: gimmieyouretoes
Username: gimmieyouretoes
Bio: Superhero
Last Seen: 2024-09-09T00:26:10
Banner Url Landscape: https://lh3.googleusercontent.com/QwAdssB702cWAzuIYKRTM3dXRR4BzdHTm6pZ-Rmmq-6QJMZz2CuCbrGrObTmM4fGnmR6zekf7V7ZzRFf

---

MICROSOFT

Registered: true
Id: E53D1A1A77FA3A54
Name: SHDWS LUVS U 123
Location: US
Last Seen: 2024-09-06T20:58:19.970000+00:00
Creation Date: 2020-06-30T17:43:45.683000+00:00

PINTEREST

Registered: true

TEAMS

Registered: true
Id: 8:live:.cid.e53d1a1a77fa3a54
Name: SHDWS LUVS U 123
First Name: SHDWS LUVS U
Last Name: 123
Email: stephaniemartin5412@gmail.com
Cid: E53D1A1A77FA3A54
Mri: 8:live:.cid.e53d1a1a77fa3a54
User Principal Name: live:.cid.e53d1a1a77fa3a54
Type: TFLUser

DROPBOX

Registered: true
Id: dbid:AAAlEYsZ3T50iOz5db8sMXjPhcdbhDywNRk
Name: stephanie martin
First Name: stephanie
Last Name: martin
Email: stephaniemartin5412@gmail.com
Verified: true

EA

Registered: true

MAPS

Profile Url

Registered: true
Private: false

GOOGLE

Picture Url

Registered: true
Id: 110665661200830022998
Name: Stephanie Martin
Last Seen: 2024-09-14T18:19:56

AIRBNB

Picture Url

Registered: true
First Name: Stephanie

EBAY

Picture Url
Profile Url

Registered: true
First Name: stephanie
Location: United States
Username: stephanimarti-975
Phone Hint: 2xx-xxx-xx96
Creation Date: 2016-11-15T00:00:00
Feedbacks Url: https://www.ebay.com/fdbk/feedback_profile/stephanimarti-975
Positive Feedback: 0
Neutral Feedback: 0
Negative Feedback: 0
Feedback Received: 8
Auth Providers: Google

YELP

Profile Url

Registered: true
Id: sEBbzSrbZ4dUlI4rUc1h7Q
Name: Stephanie M.

First Name: Stephanie
Location: Derby, CT
Followers: 0
Following: 0
Creation Date: 2017-12-18T00:19:15
Name Without Period: Stephanie M
Name With Nickname: Stephanie M.
Share Url: https://www.yelp.com/user_details?userid=sEBbzSrbZ4dUlI4rUc1h7Q&utm_source=ishare
Last Initial: M
Review Count: 1
Check In Count: 0
Quicktip Count: 0
Regular Count: 0
Weekly Check In Count: 0
Thanx Count: 0
Business Photo Count: 0
User Photo Count: 0
First To Tip Count: 0
First To Review Count: 0
Video Count: 0
Moment Count: 0
Business Answer Count: 0
Business Question Count: 0
Follower Count: 0
Badge Count: 0
Weekly Check In Rank: 59303
Friend Check In Rank: 1
Friend Active Count: 0
Fmode: 0

PAYPAL

Registered: true
Phone Hint: +1 2**-***-0396
Acc Number: 1687********9088
