Report for: colebostonsmom@yahoo.com

As of 2024-07-29T02:50:51.633Z

Minified and concise search report.

Module Responses:

PINTEREST

Registered: true

DISNEYSTORE

Registered: true

DISQUS

Registered: true

FACEBOOK

Registered: true

MEDIUM

Picture Url
Profile Url

Registered: true
Id: 7020c5fabf00
Name: Jennifer Marsh-Altman
Username: jennifermarshaltman

Followers: 7
Following: 9
Premium: false
Membership Date: 0
Authored Books: 0

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://haveibeenpwned.com/Content/Images/PwnedLogos/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
Breach Count: 361468099

HIBP

Picture Url

Registered: true
Breach: true
Name: Coupon Mom / Armor Games
Bio: In 2014, a file allegedly containing data hacked from Coupon Mom was created and included 11 million email addresses and plain text passwords. On further investigation, the file was also found to contain data indicating it had been sourced from Armor Games. Subsequent verification with HIBP subscribers confirmed the passwords had previously been used and many subscribers had used either Coupon Mom or Armor Games in the past. On disclosure to both organisations, each found that the data did not represent their entire customer base and possibly includes records from other sources with common subscribers. The breach has subsequently been

flagged as "unverified" as the source cannot be emphatically proven. In July 2020, the data was also found to contain BeerAdvocate accounts sourced from a previously unknown breach.

Creation Date: 2014-02-08T00:00:00

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

Description: In 2014, a file allegedly containing data hacked from Coupon Mom was created and included 11 million email addresses and plain text passwords. On further investigation, the file was also found to contain data indicating it had been sourced from Armor Games. Subsequent verification with HIBP subscribers confirmed the passwords had previously been used and many subscribers had used either Coupon Mom or Armor Games in the past. On disclosure to both organisations, each found that the data did not represent their entire customer base and possibly includes records from other sources with common subscribers. The breach has subsequently been flagged as "unverified" as the source cannot be emphatically proven. In July 2020, the data was also found to contain BeerAdvocate accounts sourced from a previously unknown breach.

Title: Coupon Mom / Armor Games

Breach Count: 11010525

HIBP

Picture Url

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

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

Description: 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.

Title: Data Enrichment Exposure From PDL Customer

Breach Count: 622161052

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://haveibeenpwned.com/Content/Images/PwnedLogos/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
Breach Count: 593427119

HIBP

Picture Url

Registered: true
Breach: true
Name: LinkedIn
Website: linkedin.com
Bio: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. 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, LinkedIn had 164 million email addresses and passwords exposed. 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: MyHeritage
Website: myheritage.com
Bio: In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 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 be attributed to "BenjaminBlue@exploit.im".
Creation Date: 2017-10-26T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/MyHeritage.png
Website: myheritage.com
Description: In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 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 be attributed to "BenjaminBlue@exploit.im".
Title: MyHeritage
Breach Count: 91991358

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://haveibeenpwned.com/Content/Images/PwnedLogos/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
Breach Count: 359420698

HIBP

Picture Url

Registered: true
Breach: true
Name: Not Acxiom
Bio: In 2020, a corpus of data containing almost a quarter of a billion records spanning over 400 different fields was misattributed to database marketing company Acxiom and subsequently circulated within the hacking community. On review, Acxiom concluded that "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". 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 corpus of data containing almost a quarter of a billion records spanning over 400 different fields was misattributed to database marketing company Acxiom and subsequently circulated within the hacking community. On review, Acxiom concluded that "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". The data contained almost 52M unique email addresses.
Title: Not Acxiom
Breach Count: 51730831

HIBP

Picture Url

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
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Poshmark.png
Website: poshmark.com
Description: 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".
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 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://haveibeenpwned.com/Content/Images/PwnedLogos/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
Breach Count: 393430309

HIBP

Picture Url

Registered: true
Breach: true
Name: Twitter (200M)
Website: twitter.com
Bio: In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. 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, over 200M records scraped from Twitter appeared on a popular hacking forum. 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 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://haveibeenpwned.com/Content/Images/PwnedLogos/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
Breach Count: 763117241

HIBP

Picture Url

Registered: true
Breach: true
Name: You've Been Scraped
Bio: In October and November 2018, security researcher Bob Diachenko identified several unprotected MongoDB instances believed to be hosted by a data aggregator. Containing a total of over 66M records, the owner of the data couldn't be identified but it is believed to have been scraped from LinkedIn hence the title "You've Been Scraped". The exposed records included names, both work and personal email addresses, job titles and links to the individuals' LinkedIn profiles.

Creation Date: 2018-10-05T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/List.png
Description: In October and November 2018, security researcher Bob Diachenko identified several unprotected MongoDB instances believed to be hosted by a data aggregator. Containing a total of over 66M records, the owner of the data couldn't be identified but it is believed to have been scraped from LinkedIn hence the title "You've Been Scraped". The exposed records included names, both work and personal email addresses, job titles and links to the individuals' LinkedIn profiles.
Title: You've Been Scraped
Breach Count: 66147869

HIBP

Picture Url

Registered: true
Breach: true
Name: Zynga
Website: zynga.com
Bio: In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.
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 Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.
Title: Zynga
Breach Count: 172869660

ESPN

Registered: true

INSTAGRAM

Registered: true

REDFIN

Registered: true

APPLE

Registered: true

FOURSQUARE

Picture Url
Profile Url

Registered: true
Id: 23268829
First Name: Jennifer
Last Name: Altman
Gender: female
Location: MA
Username: jennifea5510721
Private: false
Home City: MA

TWITTER

Registered: true

GIPHY

Registered: true

NOTION

Registered: true
Id: a5cca97a-be43-4df5-a487-b78bec2d1158
Version: 1
Role: reader

MICROSOFT

Registered: true
Id: E02A55609C1E711F
Name: Jennifer altman
Location: US
Last Seen: 2019-06-23T21:54:41.890000+00:00
Creation Date: 2015-11-12T22:38:09.423000+00:00

PANDORA

Picture Url
Profile Url

Registered: true
Username: colebostonsmom
Followers: 0
Following: 0
Likes: 0
Stations: 11

VIVINO

Picture Url
Profile Url
Banner Url

Registered: true
Id: 13488427
Name: Jennifer Marsh-Altman

Language: en
Location: us
Username: jennifer-marsh-
Followers: 0
Following: 0
Premium: false
Private: false
Visibility: all

MYSPACE

Registered: true

EA

Registered: true

CYBERBACKGROUNDCHECKS

Registered: true
Name: Jennifer A Altman
Age: 53
Location: 500 Indian Lake Shore Dr, Hudson, MA, 01749, US
Email: jenaltman022@icloud.com, hipn8500@eudoramail.com, jenhipner@hotmail.com, jenniferaltman656@gmail.com, colebostonsmom@yahoo.com, patrickrevelesjohn@gmail.com, jrosajunior@aol.com, sixinchsmall@aol.com, jennifer.altman@genesishcc.com, jenhipner@netzero.com, jennifer.altman@genesishcc.con
Phone: (508) 329-1517, (508) 836-0218, (978) 284-0629, (508) 254-2488, (508) 251-2733, (508) 485-5672, (503) 668-5772
Other Names: Jennifer Altman, Jennifer A Hipner, Jennifer A Marsh, Jen Altman, Jennifer Hipner, Jenny A Altman, Jennifer J Marsh, Jennifer Marsh, Jenny Altman
Results Page: https://www.cyberbackgroundchecks.com/detail/jennifer-a-altman/pidnblqyaplxgxlymxmalm

---

YELP

Picture Url

Profile Url

Registered: true
Id: JoVuAC74ohXV6cmdDGpJQA
Name: Jennifer M.
First Name: Jennifer
Gender: f
Location: Westborough, MA
Followers: 49
Following: 0
Creation Date: 2016-12-02T03:36:26
Name Without Period: Jennifer M
Name With Nickname: Jennifer M.
Share Url: https://www.yelp.com/user_details?userid=JoVuAC74ohXV6cmdDGpJQA&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: 1
User Photo Count: 1
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
Friend Check In Rank: 10
Friend Active Count: 6
Fmode: 0
