Report for: david@baszucki.com

As of 2025-08-13T23:45:24.210Z

Minified and concise search report.

Module Responses:

REPLIT

Registered: true

TAGGED

Registered: true

ESPN

Registered: true

GOODREADS

Picture Url
Profile Url

Registered: true
Id: 39009052
Name: David Baszucki
Friends Count: 0
Review Count: 1

ADOBE

Registered: true
Status: active
Type: individual

FACEBOOK

Registered: true
Email Hint: d*****@r*******.com

NOTION

Registered: true
Id: 2c7beac1-43fe-4952-a082-aa14904b965d
Version: 1
Role: reader

NEXTDOOR

Registered: true

SPIRIT

Registered: true
Id: 0
Name: DAVID BASZUCKI
First Name: DAVID
Last Name: BASZUCKI
Zip: 94028

PINTEREST

Registered: true

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: 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: B2B USA Businesses
Bio: In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.
Creation Date: 2017-07-18T00:00:00
Logo: https://logos.haveibeenpwned.com/Email.png
Description: In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.
Title: B2B USA Businesses
Modified Date: 2017-07-18T07:38:04Z
Breach Count: 105059554

HIBP

Picture Url

Registered: true
Breach: true
Name: Onliner Spambot
Bio: In August 2017, a spambot by the name of <a href="https://benkowlab.blogspot.com.au/2017/08/from-onliner-spambot-to-millions-of.html" target="_blank"

rel="noopener">Onliner Spambot was identified by security researcher Benkow mo u qa. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Creation Date: 2017-08-28T00:00:00

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

Description: In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow mo u qa. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Title: Onliner Spambot

Modified Date: 2017-08-29T19:25:56Z

Breach Count: 711477622

HIBP

Picture Url

Registered: true

Breach: true

Name: Ticketfly

Website: ticketfly.com

Bio: In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, Ticketfly later issued an incident update and stated that "It is possible, however, that hashed values of password credentials could have been accessed".

Creation Date: 2018-05-31T00:00:00

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

Website: ticketfly.com

Description: In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken

offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, Ticketfly later issued an incident update and stated that "It is possible, however, that hashed values of password credentials could have been accessed".

Title: Ticketfly

Modified Date: 2021-07-23T03:15:33Z

Breach Count: 26151608

HIBP

Picture Url

Registered: true

Breach: true

Name: Exactis

Website: exactis.com

Bio: In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.

Creation Date: 2018-06-01T00:00:00

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

Website: exactis.com

Description: In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.

Title: Exactis

Modified Date: 2018-07-25T20:00:44Z

Breach Count: 131577763

HIBP

Picture Url

Registered: true
Breach: true
Name: Apollo
Website: apollo.io
Bio: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.
Creation Date: 2018-07-23T00:00:00
Logo: https://logos.haveibeenpwned.com/Apollo.png
Website: apollo.io
Description: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.
Title: Apollo
Modified Date: 2018-10-23T04:01:48Z
Breach Count: 125929660

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://logos.haveibeenpwned.com/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

Modified Date: 2018-12-06T19:11:27Z

Breach Count: 66147869

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: Wanelo
Website: wanelo.com
Bio: In approximately December 2018, the digital mall Wanelo suffered a data breach. The data was later placed up for sale on a dark web marketplace along with a collection of other data breaches in April 2019. A total of 23 million unique email addresses were included in the breach alongside passwords stored as either MD5 or bcrypt hashes. After the initial HIBP load, further data containing names, shipping addresses and IP addresses were also provided to HIBP, albeit without direct association to the email addresses and passwords.
Creation Date: 2018-12-13T00:00:00
Logo: https://logos.haveibeenpwned.com/Wanelo.png
Website: wanelo.com
Description: In approximately December 2018, the digital mall Wanelo suffered a data breach. The data was later placed up for sale on a dark web marketplace along with a collection of other data breaches in April 2019. A total of 23 million unique email addresses were included in the breach alongside passwords stored as either MD5 or bcrypt hashes. After the initial HIBP load, further data containing names, shipping addresses and IP addresses were also provided to HIBP, albeit without direct association to the email addresses and passwords.
Title: Wanelo
Modified Date: 2019-10-01T05:39:41Z
Breach Count: 23165793

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://logos.haveibeenpwned.com/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
Modified Date: 2019-11-22T20:13:04Z
Breach Count: 622161052

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://logos.haveibeenpwned.com/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
Modified Date: 2020-01-11T00:41:51Z
Breach Count: 172869660

HIBP

Picture Url

Registered: true
Breach: true
Name: NetGalley
Website: netgalley.com
Bio: In December 2020, the book promotion site NetGalley suffered a data breach. The incident exposed 1.4 million unique email addresses alongside names, usernames, physical and IP addresses, phone numbers, dates of birth and passwords stored as salted SHA-1 hashes.
Creation Date: 2020-12-21T00:00:00
Logo: https://logos.haveibeenpwned.com/NetGalley.png
Website: netgalley.com
Description: In December 2020, the book promotion site NetGalley suffered a data breach. The incident exposed 1.4 million unique email addresses alongside names, usernames, physical and IP addresses, phone numbers, dates of birth and passwords stored as salted SHA-1 hashes.
Title: NetGalley
Modified Date: 2021-11-25T22:08:12Z
Breach Count: 1436435

HIBP

Picture Url

Registered: true
Breach: true
Name: ClearVoice Surveys
Website: clearvoicesurveys.com
Bio: In April 2021, the market research surveys company ClearVoice Surveys had a publicly facing database backup from 2015 taken and redistributed on a popular hacking forum. The data included 15M unique email addresses across more than 17M rows of data that also included names, physical and IP addresses, genders, dates of birth and plain text passwords. ClearVoice Surveys advised they were aware of the breach and confirmed its authenticity.
Creation Date: 2015-08-23T00:00:00
Logo: https://logos.haveibeenpwned.com/ClearVoiceSurveys.png
Website: clearvoicesurveys.com
Description: In April 2021, the market research surveys company ClearVoice Surveys had a publicly facing database backup from 2015 taken and redistributed on a popular hacking forum.

The data included 15M unique email addresses across more than 17M rows of data that also included names, physical and IP addresses, genders, dates of birth and plain text passwords. ClearVoice Surveys advised they were aware of the breach and confirmed its authenticity.
Title: ClearVoice Surveys
Modified Date: 2021-04-23T05:00:19Z
Breach Count: 15074786

HIBP

Picture Url

Registered: true
Breach: true
Name: ParkMobile
Website: parkmobile.io
Bio: In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.
Creation Date: 2021-03-21T00:00:00
Logo: https://logos.haveibeenpwned.com/ParkMobile.png
Website: parkmobile.io
Description: In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.
Title: ParkMobile
Modified Date: 2021-04-30T03:07:24Z
Breach Count: 20949825

HIBP

Picture Url

Registered: true
Breach: true
Name: Epik
Website: epik.com
Bio: In September 2021, <a href="https://arstechnica.com/information-technology/2021/09/

anonymous-leaks-gigabytes-of-data-from-epik-web-host-of-gab-and-parler/" target="_blank" rel="noopener">the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers, physical addresses, purchases and passwords stored in various formats.

Creation Date: 2021-09-13T00:00:00

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

Website: epik.com

Description: In September 2021, the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers, physical addresses, purchases and passwords stored in various formats.

Title: Epik

Modified Date: 2021-09-19T21:27:17Z

Breach Count: 15003961

HIBP

Picture Url

Registered: true

Breach: true

Name: LinkedIn Scraped Data (2021)

Website: linkedin.com

Bio: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.

Creation Date: 2021-04-08T00:00:00

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

Website: linkedin.com

Description: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records

with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.
Title: LinkedIn Scraped Data (2021)
Modified Date: 2023-11-07T06:51:33Z
Breach Count: 125698496

HIBP

Picture Url

Registered: true
Breach: true
Name: MGM Resorts (2022 Update)
Website: mgmresorts.com
Bio: In July 2019, MGM Resorts discovered a data breach of one of their cloud services. The breach included 10.6M guest records with 3.1M unique email addresses stemming back to 2017. In May 2022, a superset of the data totalling almost 25M unique email addresses across 142M rows was extensively shared on Telegram. On analysis, it's highly likely the data stems from the same incident with 142M records having been discovered for sale on a dark web marketplace in mid-2020. The exposed data included email and physical addresses, names, phone numbers and dates of birth.
Creation Date: 2019-07-25T00:00:00
Logo: https://logos.haveibeenpwned.com/MGM.png
Website: mgmresorts.com
Description: In July 2019, MGM Resorts discovered a data breach of one of their cloud services. The breach included 10.6M guest records with 3.1M unique email addresses stemming back to 2017. In May 2022, a superset of the data totalling almost 25M unique email addresses across 142M rows was extensively shared on Telegram. On analysis, it's highly likely the data stems from the same incident with 142M records having been discovered for sale on a dark web marketplace in mid-2020. The exposed data included email and physical addresses, names, phone numbers and dates of birth.
Title: MGM Resorts (2022 Update)
Modified Date: 2022-05-29T01:43:46Z
Breach Count: 24842001

HIBP

Picture Url

Registered: true
Breach: true
Name: LinkedIn Scraped and Faked Data (2023)
Website: linkedin.com
Bio: In November 2023, a post to a popular hacking forum alleged that millions of LinkedIn records had been scraped and leaked. On investigation, the data turned out to be a combination of legitimate data scraped from LinkedIn and email addresses constructed from impacted individuals' names.
Creation Date: 2023-11-04T00:00:00
Logo: https://logos.haveibeenpwned.com/LinkedIn.png
Website: linkedin.com
Description: In November 2023, a post to a popular hacking forum alleged that millions of LinkedIn records had been scraped and leaked. On investigation, the data turned out to be a combination of legitimate data scraped from LinkedIn and email addresses constructed from impacted individuals' names.
Title: LinkedIn Scraped and Faked Data (2023)
Modified Date: 2024-06-04T19:46:37Z
Breach Count: 19788753

HIBP

Picture Url

Registered: true
Breach: true
Name: The Post Millennial
Website: thepostmillennial.com
Bio: In May 2024, the conservative news website The Post Millennial suffered a data breach. 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 thousands of mailing lists alleged 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://logos.haveibeenpwned.com/ThePostMillennial.png

Website: thepostmillennial.com
Description: In May 2024, the conservative news website The Post Millennial suffered a data breach. 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 thousands of mailing lists alleged 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
Modified Date: 2024-05-14T20:33:14Z
Breach Count: 56973345

HIBP

Picture Url

Registered: true
Breach: true
Name: National Public Data
Bio: In April 2024, a large trove of data made headlines as having exposed "3 billion people" due to a breach of the National Public Data background check service. 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 "unverified" and a full description of the incident is in the link above.
Creation Date: 2024-04-09T00:00:00
Logo: https://logos.haveibeenpwned.com/List.png
Description: In April 2024, a large trove of data made headlines as having exposed "3 billion people" due to a breach of the National Public Data background check service. 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 "unverified" and a full description of the incident is in the link above.
Title: National Public Data
Modified Date: 2024-08-13T18:09:46Z
Breach Count: 133957569

HIBP

Picture Url

Registered: true
Breach: true
Name: DemandScience by Pure Incubation
Website: demandscience.com
Bio: In early 2024, a large corpus of data from DemandScience (a company owned by Pure Incubation), appeared for sale on a popular hacking forum. Later attributed to a leak from a decommissioned legacy system, the breach contained extensive data that was largely business contact information aggregated from public sources. Specifically, the data included 122M unique corporate email addresses, physical addresses, phone numbers, employers and job titles. It also included names and for many individuals, a link to their LinkedIn profile.
Creation Date: 2024-02-28T00:00:00
Logo: https://logos.haveibeenpwned.com/DemandScience.png
Website: demandscience.com
Description: In early 2024, a large corpus of data from DemandScience (a company owned by Pure Incubation), appeared for sale on a popular hacking forum. Later attributed to a leak from a decommissioned legacy system, the breach contained extensive data that was largely business contact information aggregated from public sources. Specifically, the data included 122M unique corporate email addresses, physical addresses, phone numbers, employers and job titles. It also included names and for many individuals, a link to their LinkedIn profile.
Title: DemandScience by Pure Incubation
Modified Date: 2024-11-13T10:00:34Z
Breach Count: 121796165

HIBP

Picture Url

Registered: true
Breach: true
Name: Storenvy
Website: storenvy.com
Bio: In mid-2019, the e-commerce website Storenvy suffered a data breach that exposed millions of customer records. A portion of the breached records were subsequently posted to a hacking forum with cracked password hashes, whilst the entire corpus of 23M rows was put up for sale. The data contained 11M unique email addresses alongside usernames, IP addresses, the user's city, gender date of birth and original salted SHA-1 password hash.
Creation Date: 2019-04-04T00:00:00
Logo: https://logos.haveibeenpwned.com/Storenvy.png

Website: storenvy.com
Description: In mid-2019, the e-commerce website Storenvy suffered a data breach that exposed millions of customer records. A portion of the breached records were subsequently posted to a hacking forum with cracked password hashes, whilst the entire corpus of 23M rows was put up for sale. The data contained 11M unique email addresses alongside usernames, IP addresses, the user's city, gender date of birth and original salted SHA-1 password hash.
Title: Storenvy
Modified Date: 2025-02-16T08:31:34Z
Breach Count: 11052071

VIVINO

Picture Url
Profile Url
Banner Url

Registered: true
Id: 41651085
Name: DavidB
Language: English
Location: us
Username: jan.ellison
Followers: 1
Following: 0
Premium: false
Private: false
Visibility: all

FIREFOX

Registered: true

WHOXY

Registered: true
Website: freedomtalk.com
Creation Date: 2000-01-31T00:00:00
Registrar: Corehub, S.R.L.

WHOXY

Registered: true
Website: janmarieellison.com
Creation Date: 2009-07-12T00:00:00
Registrar: GoDaddy.com, LLC

WHOXY

Registered: true
Website: janellison.com
Creation Date: 2003-12-08T00:00:00
Registrar: GoDaddy.com, LLC

WHOXY

Registered: true
Website: baszucki.com
Creation Date: 2000-09-14T00:00:00
Registrar: Corehub, S.R.L.

DISNEY

Registered: true

EVENTBRITE

Registered: true
Id: 6244073683
Verified: true

NEWYORKTIMES

Registered: true
Id: 175069780

FITBIT

Picture Url

Registered: true
Id: 5XXZWM
Name: david b.
Type: person

BITMOJI

Registered: true

SNAPCHAT

Registered: true

DROPBOX

Picture Url

Registered: true
Id: dbid:AAAO_g9jTVWDejTC1kFWXkB-Jg42UNPho5U
Name: David Baszucki
First Name: David
Last Name: Baszucki
Verified: true
Team Id: dbtid:AAD3YdURttvCCoBHLvYSC56-YAo6zgTZ_oE

INSTACART

Registered: true

SAP

Registered: true

SPOTIFY

Registered: true

MAPS

Profile Url

Registered: true

GOOGLE

Picture Url

Registered: true
Id: 112382443569415643461
Last Seen: 2024-12-14T23:57:20

CHESS

Picture Url
Profile Url

Registered: true
Id: 31854200
First Name: David
Username: davidfun2001
Verified: false
Premium: false

Last Seen: 2024-07-26T03:34:24
Creation Date: 2016-12-24T22:28:17
Uuid: 4434b18c-ca28-11e6-8000-000000000000
Country Id: 2
Points: 0
Flair Code: nothing
Skill Level: 2
Country: United States

MICROSOFT

Registered: true
Id: 97217A4ED2ADE357
Name: David Baszucki
Location: US
Email Hint: da *** @gmail.com
Phone Hint: ********42
Last Seen: 2025-08-04T21:40:07.633000+00:00
Creation Date: 2018-10-29T00:18:34.157000+00:00

ALLTRAILS

Registered: true

STRAVA

Profile Url

Registered: true
Id: 157881555
Name: David Badzuki
First Name: David
Last Name: Badzuki
Gender: Male
Language: English
Location: United States
Followers: 1
Following: 0
Premium: false
Last Seen: 2025-02-02T05:16:48+00:00

Creation Date: 2025-02-02T05:14:59+00:00
Resource State: 3
City: San Francisco
State: California
Badge Type Id: 0
Athlete Type: 1
Date Preference: %m/%d/%Y
Measurement Preference: feet
Email Language: en-US
Starred Segment Count: 0

GITHUB

Picture Url
Profile Url

Registered: true
Id: 210294483
Username: davidbuzzu
Followers: 0
Following: 0
Last Seen: 2025-05-04T23:03:32
Creation Date: 2025-05-04T23:01:42
Platform: Github
Ssh Keys Link: https://github.com/davidbuzzu.keys
External Contributions: 0
Gists Url: https://gist.github.com/davidbuzzu

GITHUB

Picture Url
Profile Url

Registered: true
Id: 210294483
Username: davidbuzzu
Platform: Gists
Gists Nb: 0
Starred Gists Nb: 0

YELP

Profile Url

Registered: true
Id: 1bjBGEcrKgq06OaO3VpDmw
Name: David B.
First Name: David
Gender: Male
Location: San Francisco, CA
Followers: 0
Following: 0
Creation Date: 2017-06-26T19:38:05
Name Without Period: David B
Name With Nickname: David B.
Share Url: https://www.yelp.com/user_details?userid=1bjBGEcrKgq06OaO3VpDmw&utm_source=ishare
Last Initial: B
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
Friend Check In Rank: 1
Friend Active Count: 0
Fmode: 0
