Report for: mihir0786@gmail.com

As of 2024-09-23T21:09:20.081Z

Minified and concise search report.

Module Responses:

ADOBE

Registered: true
Status: active
Type: individual

SNAPCHAT

Registered: true

MYSPACE

Registered: true

GOODREADS

Picture Url
Profile Url

Registered: true
Id: 12543291
Name: Mihir Joshi
Friends Count: 15
Review Count: 0

FIREFOX

Registered: true

INSTAGRAM

Registered: true

DISQUS

Registered: true

HI5

Registered: true

FREELANCER

Registered: true

LINKEDIN

Registered: true

HIBP

Picture Url

Registered: true
Breach: true
Name: Aditya Birla Fashion and Retail

Website: abfrl.com

Bio: In December 2021, Indian retailer Aditya Birla Fashion and Retail Ltd was breached and ransomed. The ransom demand was allegedly rejected and data containing 5.4M unique email addresses was subsequently dumped publicly on a popular hacking forum the next month. The data contained extensive personal customer information including names, phone numbers, physical addresses, DoBs, order histories and passwords stored as MD5 hashes. Employee data was also dumped publicly and included salary grades, marital statuses and religions. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Creation Date: 2021-12-01T00:00:00

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

Website: abfrl.com

Description: In December 2021, Indian retailer Aditya Birla Fashion and Retail Ltd was breached and ransomed. The ransom demand was allegedly rejected and data containing 5.4M unique email addresses was subsequently dumped publicly on a popular hacking forum the next month. The data contained extensive personal customer information including names, phone numbers, physical addresses, DoBs, order histories and passwords stored as MD5 hashes. Employee data was also dumped publicly and included salary grades, marital statuses and religions. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Title: Aditya Birla Fashion and Retail

Breach Count: 5470063

HIBP

Picture Url

Registered: true

Breach: true

Name: boAt

Website: boat-lifestyle.com

Bio: In March 2024, the Indian audio and wearables brand boAt suffered a data breach that exposed 7.5M customer records. The data included physical and email address, names and phone numbers, all of which were subsequently published to a popular clear web hacking forum.

Creation Date: 2024-03-25T00:00:00

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

Website: boat-lifestyle.com

Description: In March 2024, the Indian audio and wearables brand boAt suffered a data breach that exposed 7.5M customer records. The data included physical and email address, names and phone numbers, all of which were subsequently published to a popular clear web hacking forum.

Title: boAt

Breach Count: 7528985

HIBP

Picture Url

Registered: true
Breach: true
Name: Dailymotion
Website: dailymotion.com
Bio: In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.
Creation Date: 2016-10-20T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Dailymotion.png
Website: dailymotion.com
Description: In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.
Title: Dailymotion
Breach Count: 85176234

HIBP

Picture Url

Registered: true
Breach: true
Name: Disqus
Website: disqus.com
Bio: In October 2017, the blog commenting service Disqus announced they'd suffered a data breach. The breach dated back to July 2012 but wasn't identified until years later when the data finally surfaced. The breach contained over 17.5 million unique email addresses and usernames. Users who created logins on Disqus had salted SHA1 hashes of passwords whilst users who logged in via social providers only had references to those accounts.
Creation Date: 2012-07-01T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Disqus.png
Website: disqus.com
Description: In October 2017, the blog commenting service Disqus announced they'd suffered a data breach. The breach dated back to July 2012 but wasn't identified until years later when the data finally surfaced. The breach contained over 17.5 million unique email addresses and usernames. Users who created logins on Disqus had salted SHA1 hashes of passwords

whilst users who logged in via social providers only had references to those accounts.
Title: Disqus
Breach Count: 17551044

HIBP

Picture Url

Registered: true
Breach: true
Name: Domino's India
Website: dominos.co.in
Bio: In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.
Creation Date: 2021-03-24T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Dominos.png
Website: dominos.co.in
Description: In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.
Title: Domino's India
Breach Count: 22527655

HIBP

Picture Url

Registered: true
Breach: true
Name: Dubsmash
Website: dubsmash.com
Bio: In December 2018, the video messaging service Dubsmash suffered a data breach. 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 "BenjaminBlue@exploit.im".

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 Dubsmash suffered a data breach. 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 "BenjaminBlue@exploit.im".
Title: Dubsmash
Breach Count: 161749950

HIBP

Picture Url

Registered: true
Breach: true
Name: Gaadi
Website: gaadi.com
Bio: In May 2015, the Indian motoring website known as Gaadi had 4.3 million records exposed in a data breach. The data contained usernames, email and IP addresses, genders, the city of users as well as passwords stored in both plain text and as MD5 hashes. The site was previously reported as compromised on the Vigilante.pw breached database directory.
Creation Date: 2015-05-14T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Gaadi.png
Website: gaadi.com
Description: In May 2015, the Indian motoring website known as Gaadi had 4.3 million records exposed in a data breach. The data contained usernames, email and IP addresses, genders, the city of users as well as passwords stored in both plain text and as MD5 hashes. The site was previously reported as compromised on the Vigilante.pw breached database directory.
Title: Gaadi
Breach Count: 4261179

HIBP

Picture Url

Registered: true
Breach: true

Name: IndiaMART
Website: indiamart.com
Bio: In August 2021, 38 million records from Indian e-commerce company IndiaMART were found being traded on a popular hacking forum. Dated several months earlier, the data included over 20 million unique email addresses alongside names, phone numbers and physical addresses. It's unclear whether IndiaMART intentionally exposed the data attributes as part of the intended design of the platform or whether the data was obtained by exploiting a vulnerability in the service.
Creation Date: 2021-05-23T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/IndiaMART.png
Website: indiamart.com
Description: In August 2021, 38 million records from Indian e-commerce company IndiaMART were found being traded on a popular hacking forum. Dated several months earlier, the data included over 20 million unique email addresses alongside names, phone numbers and physical addresses. It's unclear whether IndiaMART intentionally exposed the data attributes as part of the intended design of the platform or whether the data was obtained by exploiting a vulnerability in the service.
Title: IndiaMART
Breach Count: 20154583

HIBP

Picture Url

Registered: true
Breach: true
Name: Mindjolt
Website: mindjolt.com
Bio: In March 2019, the online gaming website MindJolt suffered a data breach that exposed 28M unique email addresses. Also impacted were names and dates of birth, but no passwords. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Creation Date: 2019-03-18T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Mindjolt.png
Website: mindjolt.com
Description: In March 2019, the online gaming website MindJolt suffered a data breach that exposed 28M unique email addresses. Also impacted were names and dates of birth, but no passwords. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Title: Mindjolt
Breach Count: 28364826

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: Netlog

Website: netlog.com

Bio: In July 2018, the Belgian social networking site Netlog identified a data breach of their systems dating back to November 2012 (PDF). Although the service was discontinued in 2015, the data breach still impacted 49 million subscribers for whom email addresses and plain text passwords were exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Creation Date: 2012-11-01T00:00:00

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

Website: netlog.com

Description: In July 2018, the Belgian social networking site Netlog identified a data breach of their systems dating back to November 2012 (PDF). Although the service was discontinued in 2015, the data breach still impacted 49 million subscribers for whom email addresses and plain text passwords were exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Title: Netlog

Breach Count: 49038354

HIBP

Picture Url

Registered: true
Breach: true
Name: Not SOCRadar
Bio: In August 2024, over 332M rows of email addresses were posted to a popular hacking forum. The post alleged the addresses were scraped from cybersecurity firm SOCRadar, however an investigation on their behalf concluded that "the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources". There is no suggestion the incident compromised SOCRadar's security or posed any risk to their customers. In total, the data set contained 282M unique addresses of valid email address format.
Creation Date: 2024-08-03T00:00:00
Logo: https://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 an investigation on their behalf concluded that "the actor merely utilised functionalities inherent in the platform's standard offerings, designed to gather information from publicly available sources". There is no suggestion the incident compromised SOCRadar's security or posed any risk to their customers. In total, the data set contained 282M unique addresses of valid email address format.
Title: Not SOCRadar
Breach Count: 282478425

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: Zomato
Website: zomato.com
Bio: In May 2017, the restaurant guide website Zomato was hacked resulting in the exposure of almost 17 million accounts. The data was consequently redistributed online and contains email addresses, usernames and salted MD5 hashes of passwords (the password hash was not present on all accounts). This data was provided to HIBP by whitehat security researcher and data analyst Adam Davies.
Creation Date: 2017-05-17T00:00:00
Logo: https://haveibeenpwned.com/Content/Images/PwnedLogos/Zomato.png
Website: zomato.com
Description: In May 2017, the restaurant guide website Zomato was hacked resulting in the exposure of almost 17 million accounts. The data was consequently redistributed online and contains email addresses, usernames and salted MD5 hashes of passwords (the password hash was not present on all accounts). This data was provided to HIBP by whitehat security researcher and data analyst Adam Davies.
Title: Zomato
Breach Count: 16472873

SAMSUNG

Registered: true
Phone Hint: +9198**85**38

GAANA

Registered: true

ASUS

Registered: true

APPLE

Registered: true
Phone Hint: ****** ***38

TWITTER

Registered: true

SKYPE

Picture Url

Registered: true
Id: live:.cid.cda4469eea308b85
Name: mihir joshi
Username: live:.cid.cda4469eea308b85
Contact Type: Skype4Consumer

SKYPE

Picture Url

Registered: true
Id: mihir0786
Name: mihir joshi
Location: India
Username: mihir0786
City: mumbai
Contact Type: Skype4Consumer

PINTEREST

Registered: true

MICROSOFT

Registered: true
Id: CDA4469EEA308B85
Name: mihir joshi
Location: IN
Phone Hint: ********38
Last Seen: 2024-09-23T12:40:58.600000+00:00
Creation Date: 2019-05-27T18:00:11.823000+00:00

ECONOMICTIMES

Registered: true

MAPS

Profile Url

Registered: true
Private: false

GOOGLE

Picture Url

Registered: true
Id: 106815343597683727815
Name: Mihir Joshi
Last Seen: 2024-09-19T08:59:02

GOOGLE

Registered: true
Devices: Samsung SM-N960F
Last Seen: 2024-07-23T10:17:33
Device: Samsung SM-N960F
Count: 72
Origins: Google Maps

GOOGLE

Registered: true
Devices: SONY ILCE-6000
Last Seen: 2023-03-05T12:06:05
Device: SONY ILCE-6000
Count: 15
Origins: Google Maps

GOOGLE

Registered: true
Devices: Xiaomi Redmi Note 5 Pro
Last Seen: 2022-06-10T22:11:57
Device: Xiaomi Redmi Note 5 Pro
Count: 56
Origins: Google Maps

GOOGLE

Registered: true
Devices: Canon EOS 500D
Last Seen: 2020-02-02T01:11:31
Device: Canon EOS 500D
Count: 37
Origins: Google Maps

GOOGLE

Registered: true
Devices: Apple iPhone 6 Plus
Last Seen: 2019-05-18T18:43:05
Device: Apple iPhone 6 Plus
Count: 6
Origins: Google Maps

GOOGLE

Registered: true
Devices: Xiaomi Redmi 4
Last Seen: 2018-08-27T14:13:06
Device: Xiaomi Redmi 4
Count: 7
Origins: Google Maps

GOOGLE

Registered: true
Devices: Motorola moto x4
Last Seen: 2018-07-18T14:07:00
Device: Motorola moto x4
Count: 5
Origins: Google Maps
