

Report for: kingkongjb1002@gmail.com

As of 2025-03-17T22:13:57.717Z

Minified and concise search report.

Module Responses:

ACTIVISION

Registered: true

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Verifications.io

Website: verifications.io

Bio: In February 2019, the email address validation service securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service [verifications.io](https://twitter.com/mayhemdayone) suffered a data breach. Discovered by [Bob Diachenko](https://twitter.com/mayhemdayone) and [Vinny Troia](https://twitter.com/vinnytroia), 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](https://web.archive.org/web/20190227230352/https://verifications.io/).

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 securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service [verifications.io](https://twitter.com/mayhemdayone) suffered a data breach. Discovered by [Bob Diachenko](https://twitter.com/mayhemdayone) and [Vinny Troia](https://twitter.com/vinnytroia), 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](https://web.archive.org/web/20190227230352/https://verifications.io/).

Title: Verifications.io

Modified Date: 2019-03-09T20:49:51Z

Breach Count: 763117241

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Animoto

Website: animoto.com

Bio: In July 2018, the cloud-based video making service [Animoto suffered a data breach](https://techcrunch.com/2018/08/20/animoto-hack-exposes-personal-information-geolocation-data/). The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Creation Date: 2018-07-10T00:00:00

Logo: <https://haveibeenpwned.com/Content/Images/PwnedLogos/Animoto.png>

Website: animoto.com

Description: In July 2018, the cloud-based video making service [Animoto suffered a data breach](https://techcrunch.com/2018/08/20/animoto-hack-exposes-personal-information-geolocation-data/). The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Title: Animoto

Modified Date: 2019-07-18T05:04:08Z

Breach Count: 22437749

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](https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses). 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](https://www.troyhunt.com/data-enrichment-people-data-labs-and-another-622m-email-addresses) 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](https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/) (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](https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/) (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: 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)

Modified Date: 2023-01-05T20:49:16Z

Breach Count: 211524284

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Gemplex

Website: gemplex.tv

Bio: In February 2021, the Indian streaming platform Gemplex suffered a data breach that exposed 4.6M user accounts. The impacted data included device information, names, phone numbers, email addresses and bcrypt password hashes.

Creation Date: 2021-02-18T00:00:00

Logo: <https://haveibeenpwned.com/Content/Images/PwnedLogos/Gemplex.png>

Website: gemplex.tv

Description: In February 2021, the Indian streaming platform Gemplex suffered a data breach that exposed 4.6M user accounts. The impacted data included device information, names, phone numbers, email addresses and bcrypt password hashes.

Title: Gemplex

Modified Date: 2023-12-09T02:19:40Z

Breach Count: 4563166

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: ALIEN TXTBASE Stealer Logs

Bio: In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.

Creation Date: 2025-02-15T00:00:00

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

Description: In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.

Title: ALIEN TXTBASE Stealer Logs

Modified Date: 2025-02-25T19:25:18Z

Breach Count: 284132969

SPOTIFY

Registered: true

CALLOFDUTY

Registered: true

KHANACADEMY

[Picture Url](#)

[Profile Url](#)

Registered: true

Id: kaid_870482026423350108554524

Name: kingkongjb1002

Username: kingkongjb1002

Points: 0

NEXON

Registered: true

FACEBOOK

Registered: true

APPLE

Registered: true

INSTAGRAM

Registered: true

PANDORA

[Picture Url](#)

[Profile Url](#)

Registered: true

Username: Jacobie Brannon

PAYPAL

Registered: true
Email Hint: *** 02@gm *** .com
Phone Hint: +13 *** 8236
Acc Number: 1673*****1562

PLAYGAMES

[Picture Url](#)

[Banner Url](#)

Registered: true
Id: g08213852070795034795
Name: TeflonJavelina999
Username: TeflonJavelina999
Bio: General
Last Seen: 2017-11-23T17:38:06
Banner Url Landscape: https://lh3.googleusercontent.com/
AogCtkMsMmscGAqvG5xC5h5Oy0XwlL9nlE9fq8HR2rXIRl5clnsZxnhrkqH0zlPE0AmGoe_x0WzzSck5Tb0

SAMSUNG

Registered: true

TWITTER

Registered: true

MAPS

[Profile Url](#)

Registered: true

GOOGLE

[Picture Url](#)

Registered: true
Id: 113404024700776203218
Last Seen: 2023-10-28T07:45:29

SKYPE

[Picture Url](#)

Registered: true
Id: minegammer22
Name: Jacoby
Location: United States, bossier
Username: minegammer22
Country Code: us
Country: United States
City: bossier
Contact Type: Skype4Consumer

MICROSOFT

[Picture Url](#)

Registered: true
Id: E33B952454BD406B
Name: coby bryant
Location: US
Email Hint: br *** @aol.com
Phone Hint: *****28
Last Seen: 2025-03-11T09:23:38.403000+00:00
Creation Date: 2015-04-23T22:20:33.377000+00:00
