

Report for: monimo1129@yahoo.com

As of 2025-03-02T03:09:14.702Z

Minified and concise search report.

Module Responses:

PINTEREST

Registered: true

CARE2

Registered: true

INSTAGRAM

Registered: true

HANDY

Registered: true

First Name: Monica

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Modern Business Solutions

Website: modbsolutions.com

Bio: In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.

Creation Date: 2016-10-08T00:00:00

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

Website: modbsolutions.com

Description: In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.

Title: Modern Business Solutions

Modified Date: 2016-10-12T09:09:11Z

Breach Count: 58843488

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 Special K Data Feed was discovered containing almost 31M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. Read more about spam lists in HIBP.

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 Special K Data Feed was discovered containing almost 31M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers.

Read more about spam lists in HIBP.

Title: Special K Data Feed Spam List

Modified Date: 2016-11-24T00:18:27Z

Breach Count: 30741620

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

Modified Date: 2017-03-08T23:49:53Z

Breach Count: 393430309

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Onliner Spambot

Bio: 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.

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

Logo: <https://haveibeenpwned.com/Content/Images/PwnedLogos/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: ShareThis

Website: sharethis.com

Bio: In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and 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 dehashed.com.

Creation Date: 2018-07-09T00:00:00

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

Website: sharethis.com

Description: In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and 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 dehashed.com.

rel="noopener">dehashed.com.

Title: ShareThis

Modified Date: 2019-03-12T21:00:14Z

Breach Count: 40960499

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

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

Breach Count: 763117241

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Evite

Website: evite.com

Bio: In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Creation Date: 2013-08-11T00:00:00

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

Website: evite.com

Description: In April 2019, the social planning website for managing online invitations Evite identified a data breach of their systems. Upon investigation, they found unauthorised access to a database archive dating back to 2013. The exposed data included a total of 101 million unique email addresses, most belonging to recipients of invitations. Members of the service also had names, phone numbers, physical addresses, dates of birth, genders and passwords stored in plain text exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Title: Evite

Modified Date: 2019-07-14T14:51:51Z

Breach Count: 100985047

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Unverified Data Source

Website: astoriacompany.com

Bio: In January 2021, over 11M unique email addresses were discovered by Night Lion Security alongside an extensive amount of personal information including names, physical and IP addresses, phone numbers and dates of birth. Some records also contained social security numbers, driver's license details, personal financial information and health-related data, depending on where the information was sourced from. Initially attributed to Astoria Company, they subsequently investigated the incident and confirmed the data did not originate from their services.

Creation Date: 2021-01-26T00:00:00

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

Website: astoriacompany.com

Description: In January 2021, over 11M unique email addresses were discovered by Night Lion Security alongside an extensive amount of personal information including names, physical and IP addresses, phone numbers and dates of birth. Some records also contained social security numbers, driver's license details, personal financial information and health-related data, depending on where the information was sourced from. Initially attributed to Astoria Company, [they](https://astoriacompany.com/cyber-update/) subsequently investigated the incident and confirmed the data did not originate from their services.

Title: Unverified Data Source

Modified Date: 2021-04-12T22:58:35Z

Breach Count: 11498146

HIBP

[Picture Url](#)

Registered: true

Breach: true

Name: Truth Finder

Website: truthfinder.com

Bio: In 2019, the public records search service [TruthFinder](https://www.truthfinder.com/security-incident-alert/) suffered a data breach that later came to light in early 2023. The data included over 8M unique customer email addresses, names, phone numbers and passwords stored as script hashes.

Creation Date: 2019-04-12T00:00:00

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

Website: truthfinder.com

Description: In 2019, the public records search service [TruthFinder](https://www.truthfinder.com/security-incident-alert/) suffered a data breach that later came to light in early 2023. The data included over 8M unique customer email addresses, names, phone numbers and passwords stored as script hashes.

Title: Truth Finder

Modified Date: 2023-02-04T07:02:52Z

Breach Count: 8159573

FACEBOOK

Registered: true

DISNEY

Registered: true

ESPN

Registered: true

SAMSUNG

Registered: true

DROPBOX

Registered: true

Id: dbid:AAD4hXZKAJh14Mvh_nsyDEU4DRLxMXZUuwE

Name: Monica Arnett

First Name: Monica

Last Name: Arnett

Verified: true
