

OSINT Industries

Report for: **carabelli.lauren@gmail.com**

As of **2025-03-13T20:33:00.782Z**

[Map](#) • [Modules](#) • [Timeline](#)

Module Responses

GOOGLE

Registered : true

Id : 114081080848946723099

Last Seen : 2024-08-30T22:44:22



Registered : true

Devices : Canon EOS 5D Mark IV

Last Seen : 2022-07-22T13:27:51

AIRBNB

Registered : true

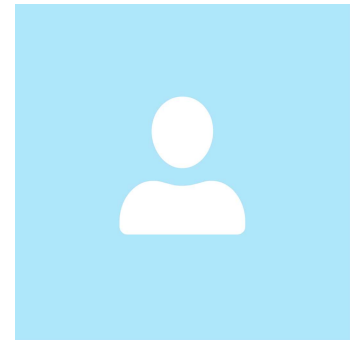
First Name : Lauren

Phone Hint : +1 ***-***-8508



SKYPE

Registered : true
Id : live:carabelli.lauren
Name : Lauren Carabelli
Username : live:carabelli.lauren



FACEBOOK

Registered : true
Phone Hint : +*****08

FITBIT

Registered : true
Id : 8TV6SZ
Name : Lauren C.



TRELLO

Registered : true
Id : 5a66257549de494efb382334
Name : Lauren Carabelli
Username : laurencarabelli
Profile Url : <https://trello.com/u/laurencarabelli>
Last Seen : 2018-01-22T17:55:01.889000+00:00

LINKEDIN

Registered : true
Id : urn:li:person:DgHqbjXC8pIf9WVfQik6vF6PyA_RPTANI3MTtOIhg6M
Name : Lauren Carabelli
First Name : Lauren
Last Name : Carabelli
Language : en (us)
Location : Hingham, Massachusetts, United States
Username : laurencarabelli
Profile Url : <https://linkedin.com/in/laurencarabelli>
Bio : Real Estate Agent at Compass | Instructor at The Bar Method
Private : true



HIBP

Registered : true
Breach : true
Name : Onliner Spambot
Bio : In August 2017, a spambot by the name of <https://benkowlab.blogspot.com.au/2017/08/from-onliner-spambot-to-millions-of.html> was identified by security researcher Benkow [moxu3q](https://benkowlab.blogspot.com.au/2017/08/from-onliner-spambot-to-millions-of.html). 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 <https://www.troyhunt.com/inside-the-massive-711-million-record-onliner-spambot-dump> Inside the Massive 711 Million Record Onliner Spambot Dump.

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



Registered : true
Breach : true
Name : MyFitnessPal
Website : myfitnesspal.com
Bio : In February 2018, the diet and exercise service <https://content.myfitnesspal.com/security-information/FAQ.html> MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/ 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 : 2018-02-01T00:00:00

Registered : true

Breach : true

Name : Houzz

Website : houzz.com

Bio : In mid-2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by dehashed.com.

Creation Date : 2018-05-23T00:00:00



Registered : true

Breach : true

Name : HauteLook

Website : hautelook.com

Bio : In mid-2018, the fashion shopping site HauteLook was among a raft of sites that were breached and their data then sold in early-2019. The data included over 28 million unique email addresses alongside names, genders, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Creation Date : 2018-08-07T00:00:00

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. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Creation Date : 2018-12-13T00:00:00

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

Registered : true

Breach : true

Name : Minted

Website : minted.com

Bio : In May 2020, the online marketplace for independent artists Minted suffered a data breach that exposed 4.4M unique customer records subsequently sold on a dark web marketplace. Exposed data also included names, physical addresses, phone numbers and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

Creation Date : 2020-05-06T00:00:00

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



Registered : true

Breach : true

Name : Eye4Fraud

Website : eye4fraud.com

Bio : In February 2023, data alleged to have been taken from the fraud protection service Eye4Fraud was listed for sale on a popular hacking forum. Spanning tens of millions of rows with 16M unique email addresses, the data was spread across 147 tables totalling 65GB and included both direct users of the service and what appears to be individuals who'd placed orders on other services that implemented Eye4Fraud to protect their sales. The data included names and bcrypt password hashes for users, and names, phone numbers, physical addresses and partial credit card data (card type and last 4 digits) for orders placed using the service. Eye4Fraud did not respond to multiple attempts to report the incident.

Creation Date : 2023-01-25T00:00:00



Registered : true

Breach : true

Name : Luxottica

Website : luxottica.com

Bio : In March 2021, the world's largest eyewear company <a

href="https://www.bleepingcomputer.com/news/security/luxottica-confirms-2021-data-breach-after-info-of-70m-leaks-online/"

target="_blank" rel="noopener">Luxottica suffered a data breach via one of their partners that exposed the personal information of more than 70M

people. The data was subsequently sold via a popular hacking forum in late 2022 and included email and physical addresses, names, genders, dates of birth and phone numbers. In a statement from Luxottica, they advised they were aware of the incident and are currently
"considering other notification obligations".

Creation Date : 2021-03-16T00:00:00

Registered : true

Breach : true

Name : Naz.API

Bio : In September 2023, over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.

Creation Date : 2023-09-20T00:00:00

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

Registered : true

Breach : true

Name : Neiman Marcus

Website : neimanmarcus.com

Bio : In May 2024, the American luxury retailer Neiman Marcus suffered a data breach which was later posted to a popular hacking forum.

The data included 31M unique email addresses, names, phone numbers, dates of birth, physical addresses and partial credit card data (note: this is insufficient to make purchases). The breach was traced back to a series of attacks against the Snowflake cloud service which impacted 165 organisations worldwide.

Creation Date : 2024-04-14T00:00:00

Registered : true

Breach : true

Name : Scholastic

Website : scholastic.com

Bio : In January 2025, a data breach of the publishing company Scholastic surfaced. The breach contained 4.2M unique email addresses with many of the records also including name, phone number and physical address.

Creation Date : 2025-01-08T00:00:00

DISNEY

Registered : true

INSTACART

Registered : true

SPOTIFY

Registered : true

REDFIN

Registered : true

PINTEREST

Registered : true

BITMOJI

Registered : true

SURVEYMONKEY

Registered : true

INSTAGRAM

Registered : true

VIMEO

Registered : true

ADOBE

Registered : true

PLACEIT

Registered : true

SOLIDCORE

Registered : true

Id : 100050442

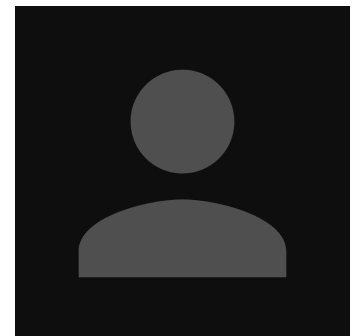
Name : Lauren Carabelli

First Name : Lauren

Last Name : Carabelli

Location : MA, Hingham

Phone : 2154998508



ESPN

Registered : true

SAMSUNG

Registered : true

HOUZZ

Registered : true

GOODREADS

Registered : true

Id : 104329764

Name : Lauren

Profile Url : <https://www.goodreads.com/user/show/104329764-lauren>



MINDBODY

Registered : true

Id : 4608022

Name : Lauren Carabelli

First Name : Lauren

Last Name : Carabelli

Verified : true

TWITTER

Registered : true

APPLE

Registered : true

Phone Hint : (***) ***-**08

STONEISUP

Registered : true

Id : 969806

Location : Studio TIU

Email : carabelli.lauren@gmail.com

ENVATO

Registered : true

MICROSOFT

Registered : true

Id : 052CBA3F24ADEB4D

Name : Lauren Carabelli

Location : US

Phone Hint : *****08

Last Seen : 2025-03-08T07:24:26.360000+00:00

Creation Date : 2018-11-13T18:40:51.137000+00:00

MAPS

Registered : true

Profile Url : <https://www.google.com/maps/contrib/114081080848946723099/reviews>

QUORA

Registered : true

Id : 1715567572

Name : Lauren Carabelli

First Name : Lauren

Last Name : Carabelli

Profile Url : <https://www.quora.com//profile/Lauren-Carabelli-1>

Followers : 0

Creation Date : 2022-01-11T19:18:54.661000



PAYPAL

Registered : true

Email Hint : *** en@gm *** .com

Phone Hint : +12 *** 8508

EBAY

Registered : true

Location : United States

Username : laucara_57

Profile Url : https://www.ebay.com/usr/laucara_57

Phone Hint : 2**-***-**08

Creation Date : 2019-02-20T00:00:00



PELOTON

Registered : true

Id : 6da657b4-a011-4037-aa78-372086209e4c

Name : Lauren Carabelli

First Name : Lauren

Last Name : Carabelli

Location : Boston

Username : LaurCara

Profile Url :

<https://members.onepeloton.com/members/LaurCara/overview>



Timeline

Content: Last Active (Trello)

Date/Year: 2018-01-22T17:55:01.889000+00:00

Content: Breached 4 times in 2018. (HaveIBeenPwnd!)

Date/Year: 2018

Content: Breached on Onliner Spambot

Date/Year: 2017-08-28T00:00:00

Content: Breached on Zynga

Date/Year: 2019-09-01T00:00:00

Content: Breached on Minted

Date/Year: 2020-05-06T00:00:00

Content: Breached on Twitter (200M)

Date/Year: 2021-01-01T00:00:00

Content: Breached on Eye4Fraud

Date/Year: 2023-01-25T00:00:00

Content: Breached on Luxottica

Date/Year: 2021-03-16T00:00:00

Content: Breached on Naz.API

Date/Year: 2023-09-20T00:00:00

Content: Breached on Combolists Posted to Telegram

Date/Year: 2024-05-28T00:00:00

Content: Breached on Neiman Marcus

Date/Year: 2024-04-14T00:00:00

Content: Breached on Scholastic

Date/Year: 2025-01-08T00:00:00

Content: Last Active (Microsoft)

Date/Year: 2025-03-08T07:24:26.360000+00:00

Content: Created Account (Microsoft)

Date/Year: 2018-11-13T18:40:51.137000+00:00

Content: Last Active (Google)

Date/Year: 2024-08-30T22:44:22

Content: Last Active (Device (Google))

Date/Year: 2022-07-22T13:27:51

Content: Created Account (Quora)

Date/Year: 2022-01-11T19:18:54.661000

Content: Created Account (Ebay)

Date/Year: 2019-02-20T00:00:00

[osint.industries](https://app.osint.industries/pdf?id=6b9fb32e-91cb-4df0-bd49-a9e67b4e81af)