

OSINT Industries

Report for: pjh3700@hotmail.com

As of **2024-06-06T09:34:25.617Z**

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

Module Responses

KHANACADEMY

Registered: true

Id: kaid_794812710005677002074438

Name: Patrick Hill

Username: X32patrick23X

Profile Url: https://www.khanacademy.org/profile/kaid_794812710005677002074438

Is Actor: false

Is Coached By Actor: false

Is Phantom: false

Points: 0



PANDORA

Registered: true

Username: pjh3700

Profile Url: <https://pandora.com/content/mobile/profile.vm?webname=pjh3700>

Followers: 0

Following: 0

Likes: 0

Stations: 12



SMULE

Registered: true

Id: 459081818

Username: X32patrick23X

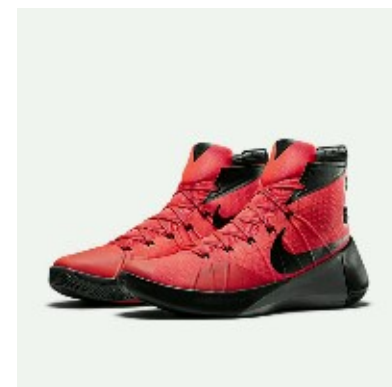
Profile Url: <https://www.smule.com/X32patrick23X>

Verified: false

Jid: 459081818@j.smule.com

Blurb:

Picture Type: user



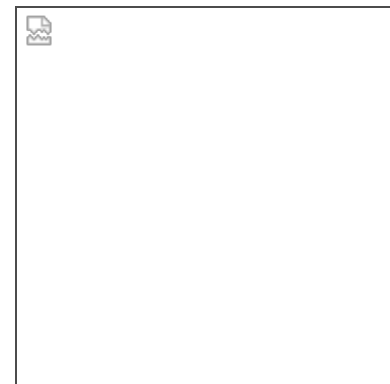
CASHAPP

Registered: true
Id: C_h4cnwqyrn
Name: Patrick Hill
Location: USA
Username: IllusiveGhost
Verified: false
Is Business: false
Is Cash Customer: true
Can Accept Payments: true



NAPSTER

Registered: true
Id: EF94CBFCD03AAC5BE040960A3803473F
Username: 4zhnjc
Followers: 0
Following: 0
Private: false
Role: member



DROPBOX

Registered: true

Id: dbid:AAAitFB1jHrOxNQjJ3J9vkpkUtbdcffqd60

Name: patrick hill

First Name: patrick

Last Name: hill

Email: pjh3700@hotmail.com

Verified: true

Disabled: false

Team Id:



PINTEREST

Registered: true

HUDSONROCK

Registered: true

Profile Url: <http://hudsonrock.com/email-search?email=pjh3700@hotmail.com>

Total Corporate Services: 0

Total User Services: 491

Computer Name: X32 Computer

Operating System: Windows 10 Home x64

Malware Path: C:\Users\X32 Computer\AppData\Local\Temp\7zS07E440CE\6248f1b75d485_Sun01af007cdc4.exe

Ip: 184.89.***.**

ADOBE

Registered: true

Type: individual

APPLE

Registered: true

Phone Hint: (???) ???-??65

Has Multiple Emails: false

VIMEO

Registered: true

IMGUR

Registered: true

TUMBLR

Registered: true

ACTIVISION

Registered: true

PORNHUB

Registered: true

SPOTIFY

Registered: true

CALLOFDUTY

Registered: true

HIBP

Registered: true

Breach: true

Name: 2,844 Separate Data Breaches

Bio: In February 2018, [a massive collection of almost 3,000 alleged data breaches was found online](#). Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.

Creation Date: 2018-02-19T00:00:00

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

Website:

Description: In February 2018, [a massive collection of almost 3,000 alleged data breaches was](#)

[found online](#). Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.

Title: 2,844 Separate Data Breaches

Breach Count: 80115532

Fabricated: false

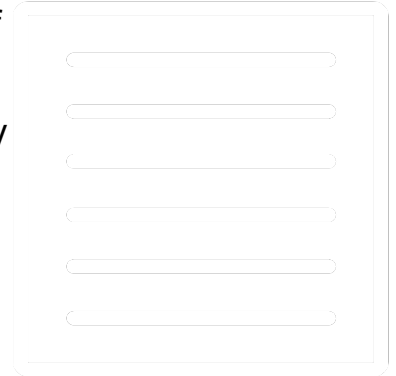
Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



Registered: true

Breach: true

Name: BlankMediaGames

Website: blankmediagames.com

Bio: In December 2018, the Town of Salem website produced by [BlankMediaGames](#) suffered a [data breach](#). Reported to HIBP by [DeHashed](#), the data contained 7.6M unique user email addresses alongside usernames, IP addresses, purchase histories and passwords stored as phpass hashes. DeHashed made multiple attempts to contact BlankMediaGames over various channels and many days but had yet to receive a response at the time of publishing.

Creation Date: 2018-12-28T00:00:00

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

Website: blankmediagames.com

Description: In December 2018, the Town of Salem website produced by [BlankMediaGames](#) suffered a data breach. Reported to HIBP by [DeHashed](#), the data contained 7.6M unique user email addresses alongside usernames, IP addresses, purchase histories and passwords stored as phpass hashes. DeHashed made multiple attempts to contact BlankMediaGames over various channels and many days but had yet to receive a response at the time of publishing.

Title: BlankMediaGames

Breach Count: 7633234

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



Registered: true

Breach: true

Name: Collection #1

Bio: In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost *2.7 billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post [The 773 Million Record "Collection #1" Data Breach](#).

Creation Date: 2019-01-07T00:00:00

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

Website:

Description: In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post [The 773 Million Record "Collection #1" Data Breach](#).

Title: Collection #1

Breach Count: 772904991

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false

Registered: true

Breach: true

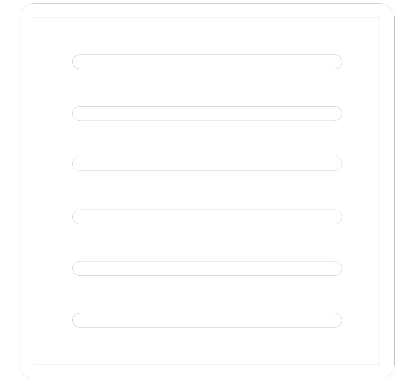
Name: Edmodo

Website: edmodo.com

Bio: In May 2017, the education platform [Edmodo was hacked](#) resulting in the exposure of 77 million records comprised of over 43 million unique customer email addresses. The data was consequently published to a popular hacking forum and made freely available. The records in the breach included usernames, email addresses and bcrypt hashes of passwords.

Creation Date: 2017-05-11T00:00:00

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



Website: edmodo.com

Description: In May 2017, the education platform [Edmodo was hacked](#) resulting in the exposure of 77 million records comprised of over 43 million unique customer email addresses. The data was consequently published to a popular hacking forum and made freely available. The records in the breach included usernames, email addresses and bcrypt hashes of passwords.

Title: Edmodo

Breach Count: 43423561

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false

Registered: true

Breach: true

Name: GameTuts

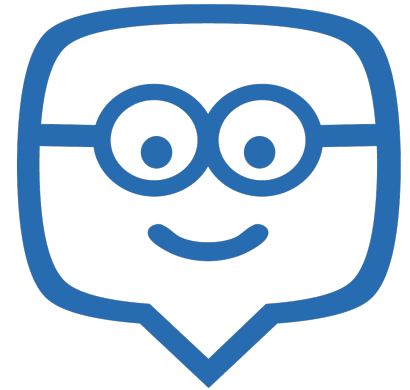
Website: game-tuts.com

Bio: Likely in early 2015, the video game website GameTuts suffered a data breach and over 2 million user accounts were exposed. The site later [shut down in July 2016](#) but was identified as having been hosted on a vBulletin forum. The exposed data included usernames, email and IP addresses and salted MD5 hashes.

Creation Date: 2015-03-01T00:00:00

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

Website: game-tuts.com



Description: Likely in early 2015, the video game website GameTuts suffered a data breach and over 2 million user accounts were exposed. The site later [shut down in July 2016](#) but was identified as having been hosted on a vBulletin forum. The exposed data included usernames, email and IP addresses and salted MD5 hashes.

Title: GameTuts

Breach Count: 2064274

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



Registered: true

Breach: true

Name: MangaDex

Website: mangadex.org

Bio: In March 2021, the manga fan site [MangaDex suffered a data breach](#) that resulted in the exposure of almost 3 million subscribers. The data included email and IP addresses, usernames and passwords stored as bcrypt hashes. The data was subsequently circulated within hacking groups.

Creation Date: 2021-03-22T00:00:00

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

Website: mangadex.org

Description: In March 2021, the manga fan site [MangaDex suffered a data breach](#) that resulted in the exposure of almost 3 million subscribers. The data included email and IP addresses, usernames and passwords stored as bcrypt hashes. The data was subsequently circulated within hacking groups.

Title: MangaDex

Breach Count: 2987329

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



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

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



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

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

Website:

Description: 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.

Title: Naz.API

Breach Count: 70840771

Fabricated: false

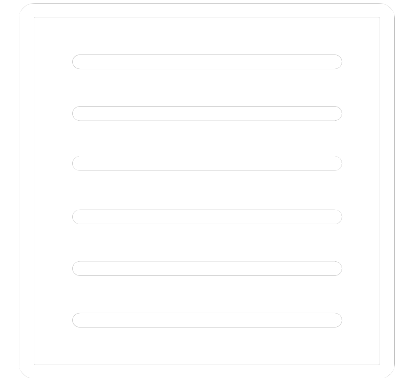
Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



Registered: true

Breach: true

Name: Teespring

Website: teespring.com

Bio: In April 2020, the custom printed apparel website [Teespring suffered a data breach that exposed 8.2 million customer records](#). The data included email addresses, names, geographic locations and social media IDs.

Creation Date: 2020-04-01T00:00:00

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

Website: teespring.com

Description: In April 2020, the custom printed apparel website [Teespring suffered a data](#)

[breach that exposed 8.2 million customer records](#). The data included email addresses, names, geographic locations and social media IDs.

Title: Teespring

Breach Count: 8234193

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



Registered: true

Breach: true

Name: Telegram Combolists

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>

Website:

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: Telegram Combolists

Breach Count: 361468099

Fabricated: false

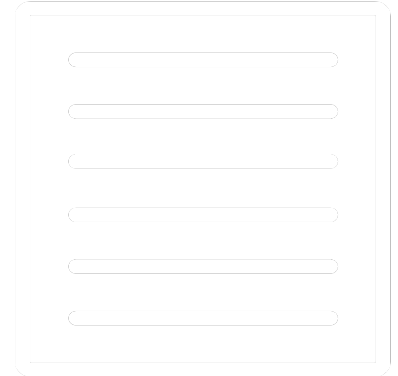
Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



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)

Breach Count: 211524284

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



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://haveibeenpwned.com/Content/Images/PwnedLogos/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

Breach Count: 172869660

Fabricated: false

Sensitive: false

Retired: false

Spam List: false

Malware: false

Subscription Free: false



Timeline

Content: Breached on Telegram Combolists (HaveIBeenPwnd!)

Start: 2024-05-28T00:00:00

Content: Breached on Naz.API (HaveIBeenPwnd!)

Start: 2023-09-20T00:00:00

Content: Breached on MangaDex (HavelBeenPwnd!)

Start: 2021-03-22T00:00:00

Content: Breached on Twitter (200M) (HavelBeenPwnd!)

Start: 2021-01-01T00:00:00

Content: Breached on Teespring (HavelBeenPwnd!)

Start: 2020-04-01T00:00:00

Content: Breached on Zynga (HavelBeenPwnd!)

Start: 2019-09-01T00:00:00

Content: Breached on Mindjolt (HavelBeenPwnd!)

Start: 2019-03-18T00:00:00

Content: Breached on Collection #1 (HavelBeenPwnd!)

Start: 2019-01-07T00:00:00

Content: Breached on BlankMediaGames (HavelBeenPwnd!)

Start: 2018-12-28T00:00:00

Content: Breached on 2,844 Separate Data Breaches (HavelBeenPwnd!)

Start: 2018-02-19T00:00:00

Content: Breached on Edmodo (HavelBeenPwnd!)

Start: 2017-05-11T00:00:00

Content: Breached on GameTuts (HavelBeenPwnd!)

Start: 2015-03-01T00:00:00

osint.industries