620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts

By Chris Williams

Published: 2019-02-11 · Archived: 2026-04-02 10:38:48 UTC

Exclusive Some 617 million online account details stolen from 16 hacked websites are on sale from today on the dark web, according to the data trove's seller.

For less than $20,000 in Bitcoin, it is claimed, the following pilfered account databases can be purchased from the Dream Market cyber-souk, located in the Tor network:

Dubsmash (162 million), MyFitnessPal (151 million), MyHeritage (92 million), ShareThis (41 million), HauteLook (28 million), Animoto (25 million), EyeEm (22 million), 8fit (20 million), Whitepages (18 million), Fotolog (16 million), 500px (15 million), Armor Games (11 million), BookMate (8 million), CoffeeMeetsBagel (6 million), Artsy (1 million), and DataCamp (700,000).

Sample account records from the multi-gigabyte databases seen by *The Register* appear to be legit: they consist mainly of account holder names, email addresses, and passwords. These passwords are hashed, or one-way encrypted, and must therefore be cracked before they can be used.

There are a few other bits of information, depending on the site, such as location, personal details, and social media authentication tokens. There appears to be no payment or bank card details in the sales listings.

Who are the buyers?

These silos of purportedly purloined information are aimed at spammers and credential stuffers, which is why copies are relatively cheap to buy. The stuffers will take usernames and passwords leaked from one site to log into accounts on other websites where the users have used the same credentials.

So, for example, someone buying the purported 500px database could decode the weaker passwords in the list, because some were hashed using the obsolete MD5 algorithm, and then try to use the email address and cracked password combinations to log into, say, strangers' Gmail or Facebook accounts, where the email address and passwords have been reused.

All of the databases are right now being touted separately by one hacker, who says he or she typically exploited security vulnerabilities within web apps to gain remote-code execution and then extract user account data. The records were swiped mostly during 2018, we're told, and went on sale this week.

The seller, who is believed to be located outside of the US, told us the Dubsmash data has been purchased by at least one person.

Some of the websites – particularly MyHeritage, MyFitnessPal, and Animoto – were known to have been hacked as they warned their customers last year that they had been compromised, whereas the others are seemingly newly disclosed security breaches. In other words, this is the first time we've heard these other sites have been allegedly hacked. This also marks the first time this data, for all of the listed sites, has been peddled publicly, again if all the sellers' claims are true.

Is this legit?

A spokesperson for MyHeritage confirmed samples from its now-for-sale database are real, and were taken from its servers in October 2017, a cyber-break-in it told the world about in 2018. ShareThis, CoffeeMeetsBagel, 8fit, 500px, DataCamp, and EyeEm also confirmed their account data was stolen from their servers and put up for sale this week in the seller's collection. This lends further credibility to the data trove.

Last week, half a dozen of the aforementioned sites were listed on Dream Market by the seller: when we spotted them, we alerted Dubsmash, Animoto, EyeEm, 8fit, Fotolog, and 500px that their account data was potentially being touted on the dark web.

Over the weekend, the underground bazaar was mostly knocked offline, apparently by a distributed denial-of-service attack. On Monday this week, the underworld marketplace returned to full strength, and the seller added the rest of the sites. We contacted all of them to alert them, and ask for a response. Meanwhile, Dream Market has been smashed offline again.

Here's a summary of what is, or briefly was, purported to be on sale:

- **Dubsmash**: 161,549,210 accounts for 0.549 BTC ($1,976) total

  11GB of data taken in December 2018. Each account record contains the user ID, SHA256-hashed password, username, email address, language, country, plus for some, but not all the users, the first and the last name. This alleged security breach has not been previously publicly disclosed. Dubsmash is a video-messaging application popular with millennials and younger folk.

  New York City-based Dubsmash has hired law firm Lewis Brisbois to probe the online sale. Partner Simone McCormick told us:

- **500px**: 14,870,304 accounts for 0.217 BTC ($780) total

  1.5GB of data taken July 2018. Each account record contains the username, email address, MD5-, SHA512- or bcrypt-hashed password, hash salt, first and last name, and if provided, birthday, gender, and city and country. 500px is a social-networking site for photographers and folks interested in photography.

  "Our engineering team is currently investigating and if we can confirm there was a breach we will take the necessary steps to inform our users as per GDPR standards," 500px spokesperson Stephanie Newell told us.

  Update: 500px staff are now notifying their users that the site was indeed hacked, and will reset everyone's passwords, starting with the ones weakly hashed using MD5.

"We are able to confirm a breach occurred," Newell told us. "Our engineers immediately launched a comprehensive review of our systems and have since taken every precaution to secure them. All areas of vulnerability have been identified and fixed during our internal investigation, and we've found no evidence to date of any recurrence of the issue.

"We are currently working on notifying our entire user base, however, given the amount of users affected, this task will span one day at minimum. We've taken every precaution to ensure our users' data is safe. A system-wide password reset is currently underway for all users, prioritized in order of accounts with the highest potential risk, and we have already forced a reset of all MD5-encrypted passwords."

In addition, 500px, which is based in Canada, said it has taken the following steps to shore up its security:

- **EyeEm**: 22,360,765 accounts for 0.289 BTC ($1,040) total

  1.7GB of data taken February 2018. Each account record contains an email address and SHA1-hashed password, although about three million are missing an email address. This security breach has not been previously publicly disclosed. Germany-based EyeEm is an online hangout for photographers. A spokesperson did not respond to a request for comment.

  Update: EyeEm has told its customers it was hacked, and forced a reset of their passwords.

- **8fit**: 20,180,667 accounts for 0.2025 BTC ($728) total

  1.9GB of data taken July 2018. Each account record contains an email address, bcrypted-hashed password, country, country code, Facebook authentication token, Facebook profile picture, name, gender, and IP address. This security breach has not been previously publicly disclosed. Germany-headquartered 8fit offers customized workout and diet plans for healthy fitness types.

  8fit CEO Aina Abiodun told us her team is investigating, adding: "I need to get back to you on this and can't comment immediately."

  Update: 8fit has confessed to its users that it was hacked, and is resetting their passwords.

- **Fotolog**: 16 million accounts for 0.52 BTC ($1,872) total

  5.9GB of data taken in December 2018. There are five SQL databases containing information including email addresses, SHA256-hashed passwords, security questions and answers, full names, locations, interests, and other profile information. This alleged security breach has not been previously publicly disclosed. Fotolog, based in Spain, is another social network for photography types. A spokesperson did not respond to a request for comment.

- **Animoto** 25,402,283 accounts for 0.318 BTC ($1,144) total

  2.1GB of data taken in 2018. Each account record contains a user ID, SHA256-hashed password, password salt, email address, country, first and last name, and date of birth. This security breach was publicly disclosed by the NYC-headquartered business in 2018, though this is the first time the data has gone on sale, we understand.

"We provided notification about an incident potentially affecting customers back in August 2018 after we identified unusual activity on our system," spokesperson Rebecca Brooks told us. "After identifying the suspicious activity, we immediately took the systems offline and implemented numerous security controls to help prevent an incident like this from happening again."

- **MyHeritage** 92,284,478 accounts for 0.549 BTC ($1,976) total

  3.6GB of data taken October 2017. Each account record contains an email address, SHA1-hashed password and salt, plus the date of account creation. This security breach was publicly disclosed by the business last year, though this is the first time the data has gone on sale, we're told. No DNA or similar sensitive information was taken. MyHeritage, based in Israel, is a family-tree-tracing service that studies customers' genetic profiles.

  A spokesperson told us:

- **MyFitnessPal** 150,633,038 accounts for 0.289 BTC ($1,040) total

  3.5GB of data taken February 2018. Each account record contains a user ID, username, email address, SHA1-hashed password with a fixed salt for the whole table, and IP address. This security breach was publicly disclosed by the business last year. This may be the first time it has gone on public sale. Under-Armor-owned MyFitnessPal does what it says on the tin: it's an app that tracks diet and exercise. A spokesperson did not respond to a request for comment.

  Update: Spokesperson Erin Wendell has told us the biz made every user reset their password following the discovery of the intrusion last year. If you reused your old MyFitnessPal password with other sites, now would be a good time to change your password on those other services, if you have not done so already.

  "We responded swiftly to alert users and have since required all MyFitnessPal users who had not changed their passwords since that March 29, 2018 announcement, to reset their passwords," Wendell said.

  "As a result, passwords previously used for MyFitnessPal at the time of the data security issue are no longer valid on MyFitnessPal, and we continue to encourage strong password practices including unique and complex passwords for all their accounts to enable users to further protect themselves."

- **Artsy** 1,070,000 accounts for 0.0289 BTC ($104) total

  184MB of data taken April 2018. Each account record contains an email address, name, IP addresses, location, and SHA512-hashed password with salt. This security breach has not been previously publicly disclosed. Artsy, located in NYC, is an online home for collecting and organizing art. A spokesperson did not respond to a request for comment.

  Update: Artsy has emailed its users to confirm its data was stolen and sold online. It is in the process of investigating how it happened.

- **Armor Games** 11,013,617 accounts for 0.2749 BTC ($988) total

1.8GB of data taken late December 2018. Each account record contains a username, email address, SHA1-hashed password and salt, date of birth, gender, location, and other profile details. This alleged security breach has not been previously publicly disclosed. California-based Armor Games is a portal for a ton of browser-based games. A spokesperson did not respond to requests for comment.

- **Bookmate** 8,026,992 accounts for 0.159 BTC ($572) total

  1.7GB of data taken July 2018. Each account record typically contains a username, an email address, SHA512 or bcrypt-hashed password with salt, gender, date of birth, and other profile details. This alleged security breach has not been previously publicly disclosed. British Bookmate makes book-reading apps. A spokesperson did not respond to a request for comment.

- **CoffeeMeetsBagel** 6,174,513 accounts for 0.13 BTC ($468) total

  673MB of data taken late 2017 and mid-2018. Each account record contains typically a full name, email address, age, registration date, and gender. This security breach has not been previously publicly disclosed. CoffeeMeetsBagel is a dating website.

  Jenn Takahashi, spokesperson for the CoffeeMeetsBagel, told us: "We are not aware of a breach at this time, but our security team is looking into this now." She also said the San-Francisco-based biz does not store passwords, and uses third-party sites for authentication.

  "We have engaged with our legal team and forensic security experts to identify any issues and ensure we have the best security stance moving forward," Takahashi added.

  Update: CoffeeMeetsBagel has confirmed at least some user account data was stolen by a hacker who broke into the biz's systems as recently as May 2018, as we reported.

  "On February 11, 2019, we learned that an unauthorized party gained access to a partial list of user details, specifically names and email addresses prior to May 2018," the company said in a statement.

  "Once we became aware, we immediately launched a comprehensive investigation with the help of experienced forensic experts. We are currently working on notifying the affected user base. The security of our users' information is important to us, and we apologize for any inconvenience this may have caused."

- **DataCamp** 700,000 accounts for 0.013 BTC ($46.8) total

  82MB of data taken December 2018. Each account record contains an email address, bcrypt-hashed password, location, and other profile details. This security breach has not been previously publicly disclosed. US-based DataCamp teaches people data science and programming. A spokesperson told us they are "looking into" the online sale.

  "We take this matter seriously and want to further verify if this is indeed the case," said the biz's Lode Vanacken. "We will also investigate access and audit logs to see if we can trace back any potential unauthorised access. If indeed further investigation shows this data to be valid we will communicate with you and with the affected end-users."

Update: Vanacken has told us DataCamp is resetting users' passwords after confirming its data was stolen. "We have notified the users we believe were affected or potentially affected via email," he said.

"Out of an abundance of caution, we are logging out all DataCamp users who may have been affected, and, if they use a password as their authentication method, we are invalidating their passwords and prompting them to reset their passwords.

"We continue to monitor for suspicious activity and to make enhancements to our systems to detect and prevent unauthorized access to user information."

- **HauteLook** 28 million accounts for 0.217 BTC ($780) total

  1.5GB of data taken during 2018. Each account record contains an email address, bcrypt-hashed password, and name. This alleged security breach has not been previously publicly disclosed. HauteLook is an online store for fashion, accessories, and so on. A spokesperson for the Los Angeles-based biz did not respond to a request for comment.

- **ShareThis** 41,028,098 accounts for 0.217 BTC ($780) total

  2.7GB of data taken early July 2018. Each account record contains a name, username, email address, DES-hashed password, gender, date of birth, and other profile info. This security breach has not been previously publicly disclosed. Palo Alto-based ShareThis makes a widget for sharing links to stuff with friends. A spokesperson did not respond to a request for comment.

  Update: ShareThis has written to its users, alerting them that the site was hacked, likely in July 2018, and that email addresses, password hashes, and some dates-of-birth was stolen and put up for sale online.

- **Whitepages** 17,775,679 accounts for 0.434 BTC ($1560) total

  2.9GB of data taken 2016. Each account record contains an email address, SHA1- or bcrypt-hashed password, and first and last name. This alleged security breach has not been previously publicly disclosed. Whitepages is a Seattle-based online telephone and address directory. A spokesperson did not respond to a request for comment.

The seller told *The Register* they have as many as 20 databases to dump online, while keeping some others back for private use, and that they have swiped roughly a billion accounts from servers to date since they started hacking in 2012.

Their aim is to make "life easier" for hackers, by selling fellow miscreants usernames and password hashes to break into other accounts, as well as make some money on the side, and highlight to netizens that they need to take security seriously – such as using two-factor authentication to protect against password theft. The thief also wanted to settle a score with a co-conspirator, by selling a large amount of private data online.

The hacker previously kept stolen databases private, giving them only to those who would swear to keep the data secret.

"I don't think I am deeply evil," the miscreant told us. "I need the money. I need the leaks to be disclosed.

"Security is just an illusion. I started hacking a long time ago. I'm just a tool used by the system. We all know measures are taken to prevent cyber attacks, but with these upcoming dumps, I'll make hacking easier than ever." ®

Updates below

This article was revised at 0430 UTC on Tuesday, February 12 to include confirmation from 500px that it was hacked, as we reported.

Also on Tuesday, EyeEm informed its users it had been hacked. We understand similar disclosures are due to land this week from ShareThis and others.

On Wednesday, February 13, DataCamp informed us it is resetting its users' passwords after "some user data was exposed by a third party who gained criminal unauthorized access to one of our systems."

Also on Wednesday, CoffeeMeetsBagel told us it is alerting its users to its security breach, we added a statement from MyFitnessPal, and 8fit admitted to its customers that it was hacked.

On Thursday, February 14, Artsy emailed its users to confirm its internal data was stolen and put up for sale, as reported. "On February 11, 2019, we became aware that account information for some of our users was made available on the internet," the biz wrote. "We are still investigating the precise causes of the incident, and together with our engineering team, we are working with a leading cyber forensics firm to assist us."

On Friday, February 15, ShareThis confirmed it was hacked, too.

On 1 March, Armor Games 'fessed up to a breach.
