# Hacker sells 22 million Unacademy user records after data breach

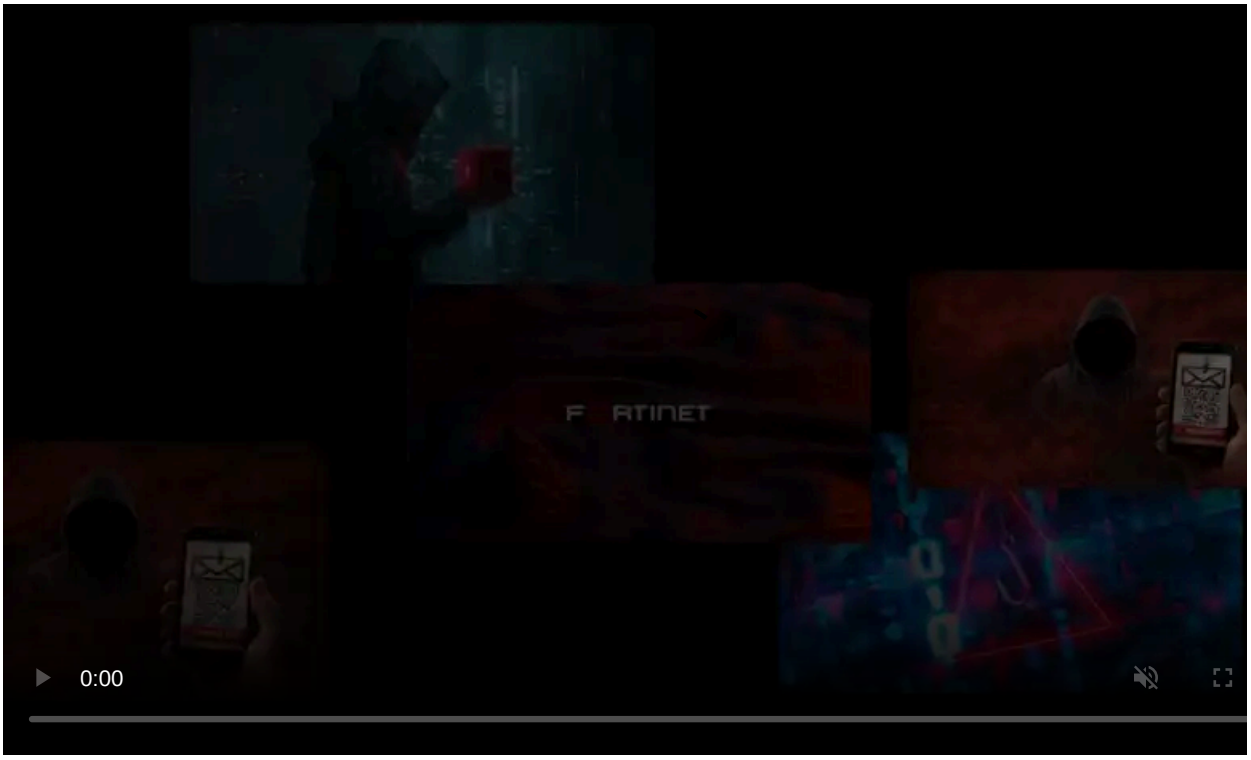
By Lawrence Abrams

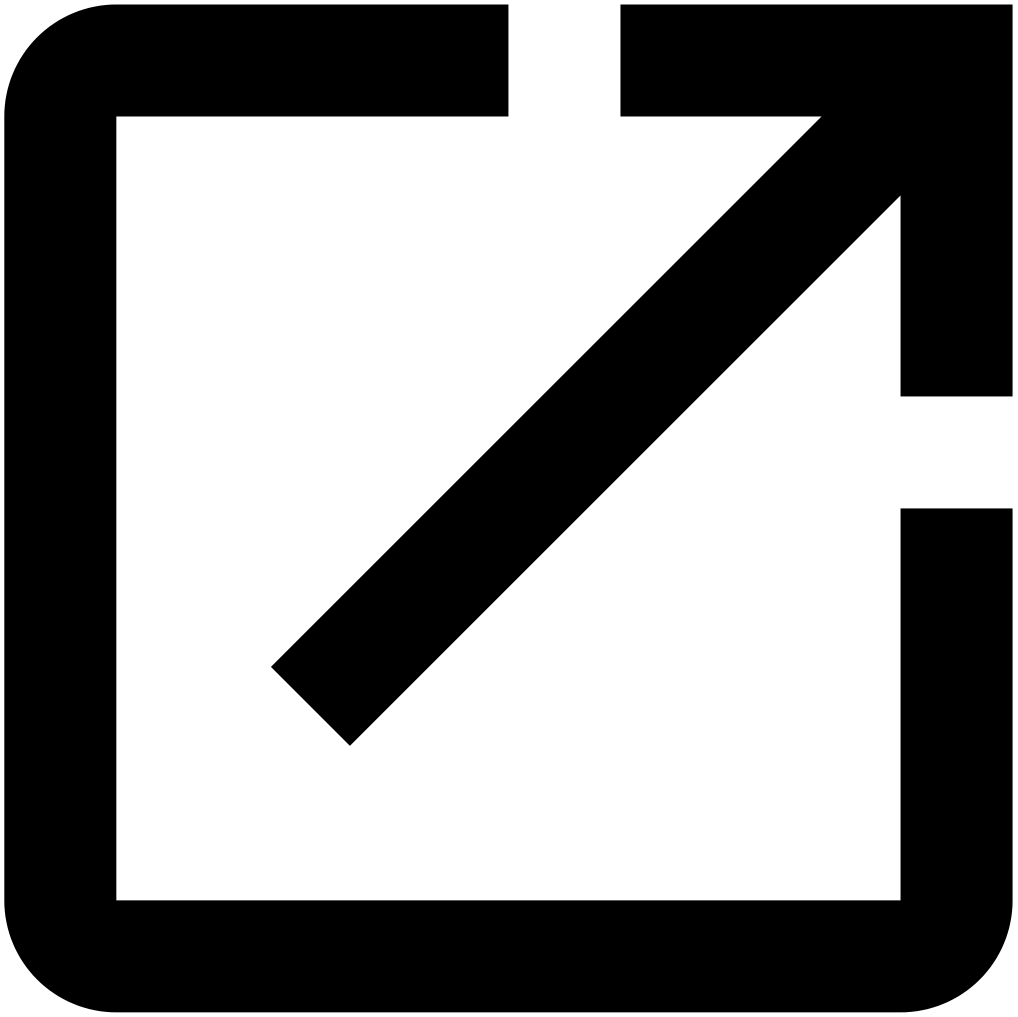
Published: 2020-05-06 · Archived: 2026-04-05 20:57:56 UTC


Online learning platform Unacademy has suffered a data breach after a hacker gained access to their database and started selling the account information for close to 22 million users.

Unacademy is one of India's largest online learning platforms boasting 14K teachers, over a million video lessons, and over 20 million registered users (learners).

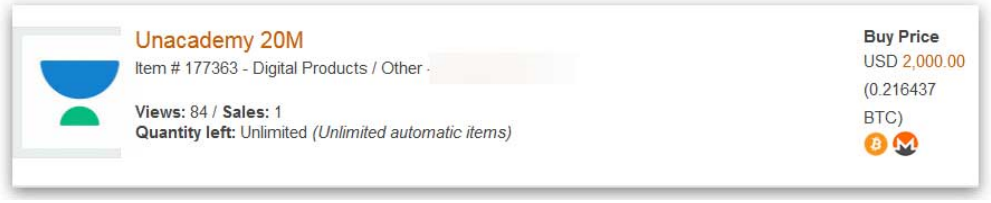
After recently raising $110 million in funding from General Atlantic, Sequoia and Facebook, Unacademy has a valuation of over $500 million.


F RTINET
0:00



## Hacker sells Unacademy user database

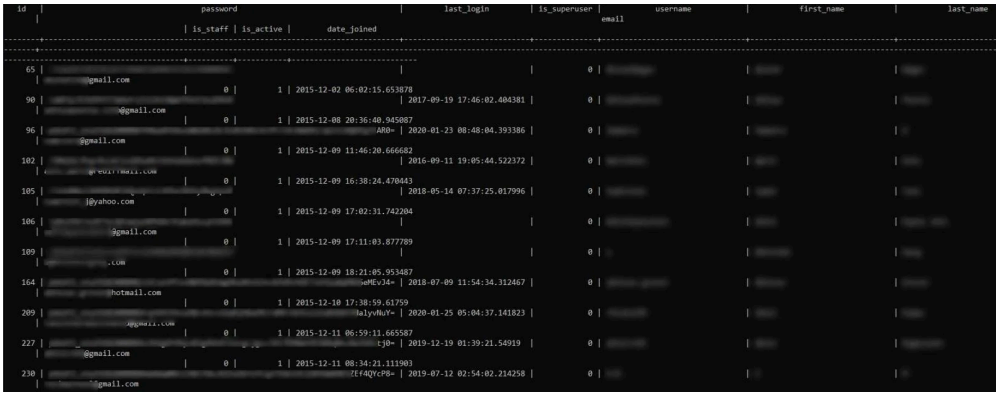
On May 3rd, 2020, cyber intelligence company Cyble Inc. discovered that a threat actor had begun to sell an Unacademy user database containing 20 million accounts for $2,000.




**Unacademy database for sale**

While advertised as 20 million, the database contains a total of 21,909,707 user records.

These records include usernames, SHA-256 hashed passwords, date joined, last login date, email addresses, first and last names, and whether the account is active, a staff member, or a superuser.




**Unacademy user records table**

After contacting numerous Unacademy users, BleepingComputer has verified that the data being sold is authentic and contains accurate information.

The last account created in the database is from January 26th, 2020, which indicates that the hacker most likely breached Unacademy's systems around that time.

Cyble has told BleepingComputer that numerous accounts using corporate emails exist in the database as well.

This includes accounts from Wipro, InfoSys, Cognizant, Google, and Facebook.

If these users utilize the same passwords on their corporate network it could allow the threat actor to gain access to these network as well.

In a statement from Hemesh Singh, Co-founder and CTO, Unacademy, confirmed the breach, but stated only 11 million users were affected and that no passwords were exposed.

"We have been closely monitoring the situation and can confirm that basic information related to around 11 million learners has been compromised. However, we would like to assure our learners that no sensitive information such as financial data, location or passwords has been breached. We follow stringent encryption methods using the PBKDF2 algorithm with a SHA256 hash, making it highly implausible for anyone to access the learner passwords. We also follow an OTP based login system that provides an additional layer of security to our learners. We are doing a complete background check and will be addressing any potential security loophole to further our efforts of ensuring a robust security mechanism. Data security and privacy of our learners is of utmost importance to us and we will be in communication with our learners to keep them updated on the progress."

As already stated, based on the samples shared with BleepingComputer, there were a far greater amount of user records exposed and they did contain hashed passwords.

BleepingComputer has once again reached out to Unacademy with follow up questions regarding these discprenacies.

## Hackers claim to have stolen more than user data

In a conversation seen by BleepingComputer, the hackers state that they have stolen much more than just the user database.

The threat actors have alleged to Cyble's researchers that they have stolen the entire database, but are only putting the user records up for sale at this time.

This holding back of other data indicates that there is more value to be had in the stolen database than just user records.

It is not known what this data includes.

## What should Unacademy users do?

If you are a registered Unacademy learner or educator, it is strongly suggested that you immediately change your password on the site.

If you use the same password at other sites, we strongly suggest that you change your password to a unique one at those sites as well.

Users should also be wary of targeted phishing emails that pretend to be from Unacademy and utilize the information stored in this database.

Cyble has acquired the database and added the user records to its data breach monitoring service amibreached.com.

Unacademy users can use this service to verify if their account was leaked as part of this breach.

**Update 5/6/20 3:42 PM EST**: Added statement

## Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---