Promo.com discloses data breach after 22M user records leaked online

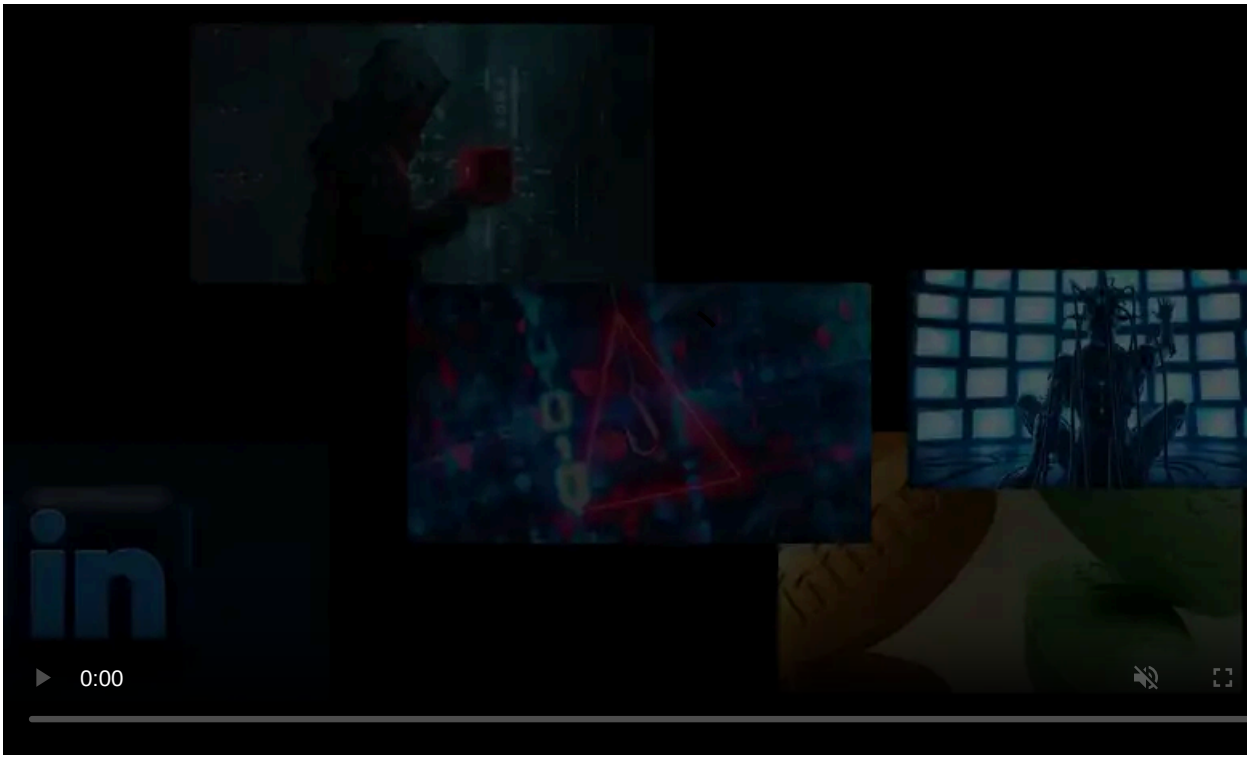
By Lawrence Abrams

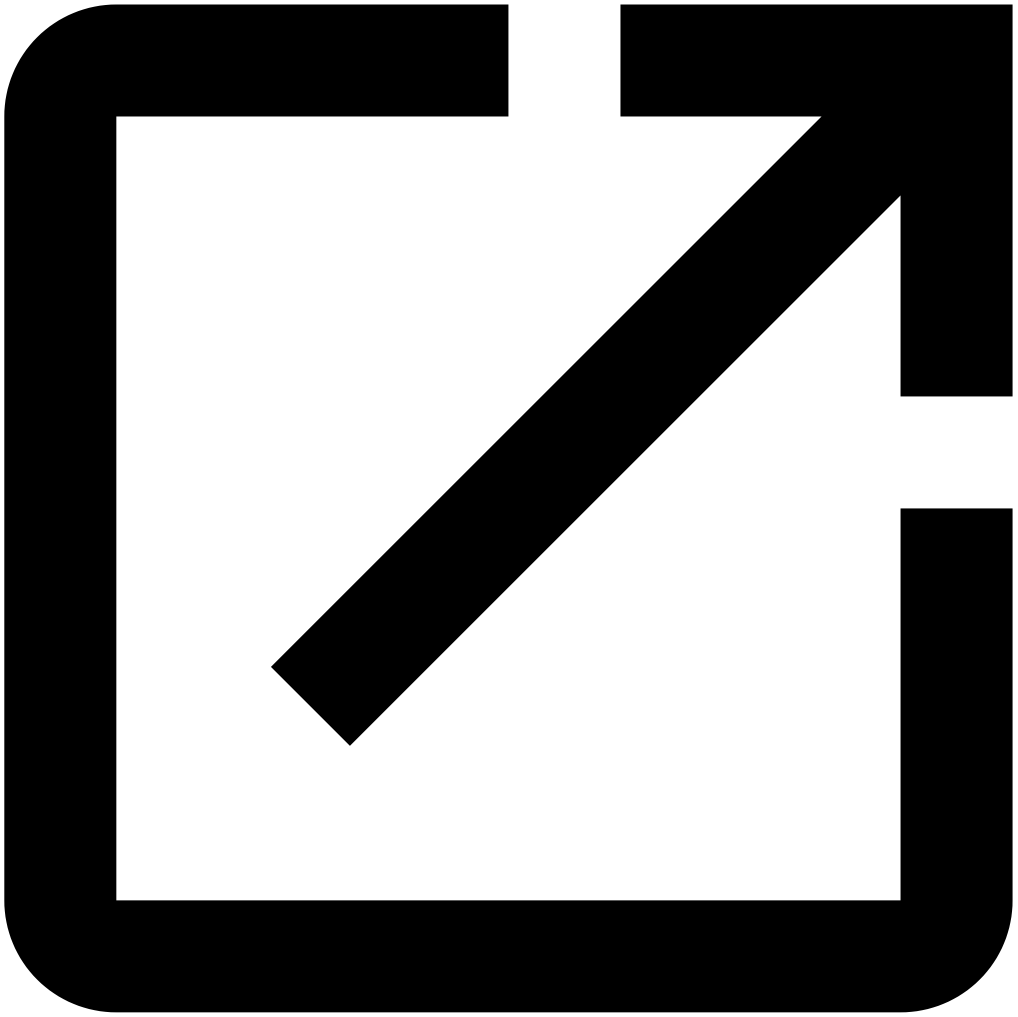
Published: 2020-07-27 · Archived: 2026-04-05 17:06:35 UTC

Promo.com, an Israeli-based marketing video creation site, has disclosed a data breach after a database containing 22 million user records was leaked for free on a hacker forum.

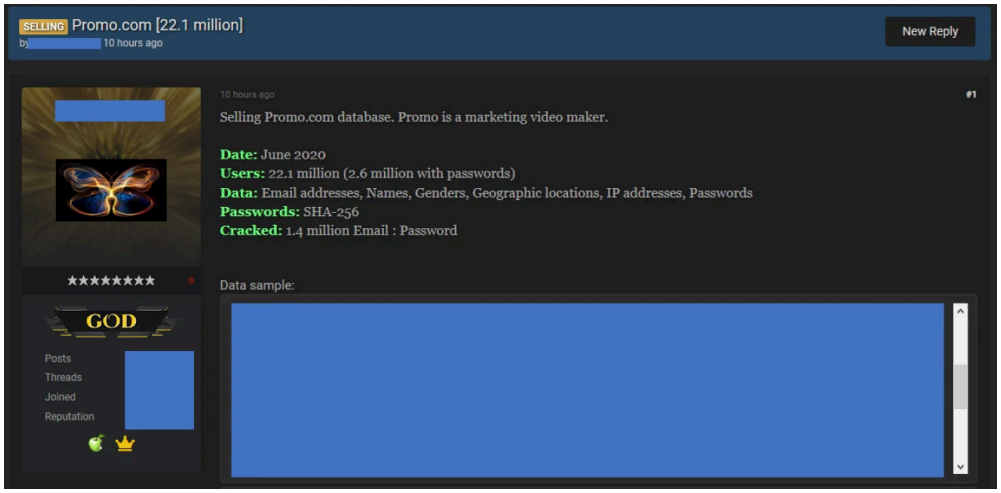
Promo is a web site that allows you to create promotional videos or ads that can then be shared on social networks such as Facebook, Instagram, Twitter, and LinkedIn.

In a report shared with BleepingComputer by cybersecurity intelligence firm CloudSEK, a well-known seller of data breaches posted a database containing 22.1 million user records on a hacker forum.


0:00



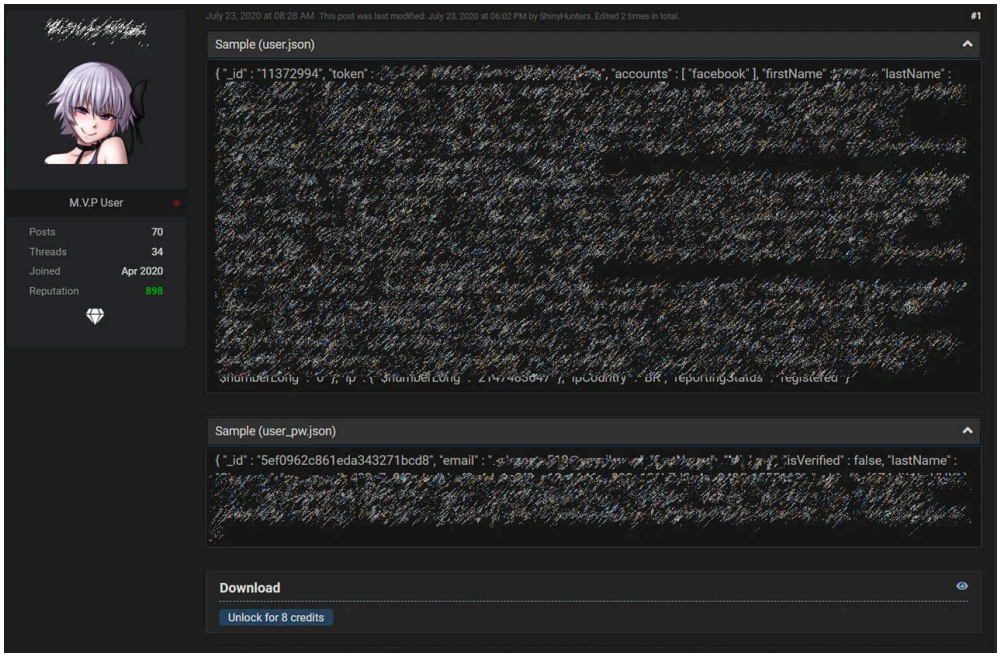
This data contains users email addresses, names, genders, geographic location, and for 2.6 million of the users, their hashed passwords.



Promo database leak

This leak included 1.4 million cracked passwords, which means they were decrypted and could immediately be used by attackers to log in to the users' accounts or use the passwords in credential stuff attacks at other sites.

This post was eventually taken down, but this past week another data breach seller released the database again on the same hacker forum.



Sample of the sold user database

It is not known if this database also contained the cracked passwords.

Promo issues data breach notification

After the public leaking of their database, Promo issued a data breach notification stating they became aware of a vulnerability on a third-party partner's service that affected their data.

"On July 21, 2020, our team became aware that a data security vulnerability on a 3rd party service had caused a breach affecting certain non-finance related Slidely and Promo user data. We immediately stopped all suspicious activity and

launched an internal investigation to further learn about what happened," Promo's data breach notification states.

Promo further stated that no financial information was exposed, but that a users IP address, gender, email address, name, and hashed and salted passwords were disclosed.

"The exposed data includes first name, last name, email address, IP address, approximated user location based on the IP address, gender, as well as encrypted, hashed and salted password to the Promo or Slidely account. Although your account password was hashed and salted (a method used to secure passwords with a key), it's possible that it was decoded," the data breach continues.

As the salt for each user's password was also included in the database, it is much easier for threat actors to crack the passwords and see them in their plain text form.

Promo also stated that "Your Log in via your social media account was not affected," but one of the databases shared on the hacker forum included social network login tokens.

It is unknown if these token can be used to log in to your social network accounts, but it is advised to regenerate the tokens if possible.

Promo is performing a mandatory reset on all affected accounts the next time they log into Promo.com.

What Promo customers should do

While the passwords leaked in this data breach were encrypted, threat actors have already started to decrypt them, and the rest can be decrypted over time.

After a user's password is cracked, threat actors would be able to use them in credential stuffing attacks at other sites.

Due to this, if you are a Promo customer, you should immediately change your password to one that is strong and unique.

If you use that same password at other sites, it is strongly advised that you change your password to a unique one at those sites as well.

A password manager can make it much easier to use unique passwords at every site and is highly recommended.

If you are concerned that you were exposed in this breach, Have I Been Pwned has added the database to their site, and you can use it to check if your record was included in the data breach.
