INNOVATION > CYBERSECURITY

16 Billion Apple, Facebook, Google And Other Passwords Leaked — Act Now

By Davey Winder, Senior Contributor. ⓘ Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Follow Author

Published Jun 19, 2025, 07:45am EDT

The biggest password leak in history confirmed.
GETTY

Update, June 19, 2025: This story, originally published on June 18, has been updated with comments from the founders of Keeper Security regarding the 16 billion leaked passwords and other login credentials across the major tech vendor landscape.

If you thought that my May 23 report, confirming the leak of login data totaling an astonishing 184 million compromised credentials, was frightening, I hope you are sitting down now. Researchers have just confirmed what is also certainly the largest data breach ever, with an almost incredulous 16 billion login credentials, including passwords, exposed. As part of an ongoing investigation that started at the beginning of the year, the researchers have postulated that the massive password leak is the work of multiple infostealers. Here's what you need to know and do.

FORBES

Amazon Issues Security Warning As Prime Account Hacks Surge

By **Davey Winder**

Is This The GOAT When It Comes To Passwords Leaking?

Password compromise is no joke; it leads to account compromise and that leads to, well, the compromise of most everything you hold dear in this technological-centric world we live in. It's why Google is telling billions of users to replace their passwords with much secure passkeys. It's why the FBI is warning people not to click on links in SMS messages. It's why stolen passwords are up for sale, in their millions, on the dark web to anyone with the very little amount of cash required to purchase them. And it's why this latest revelation is, frankly, so darn concerning for everyone.

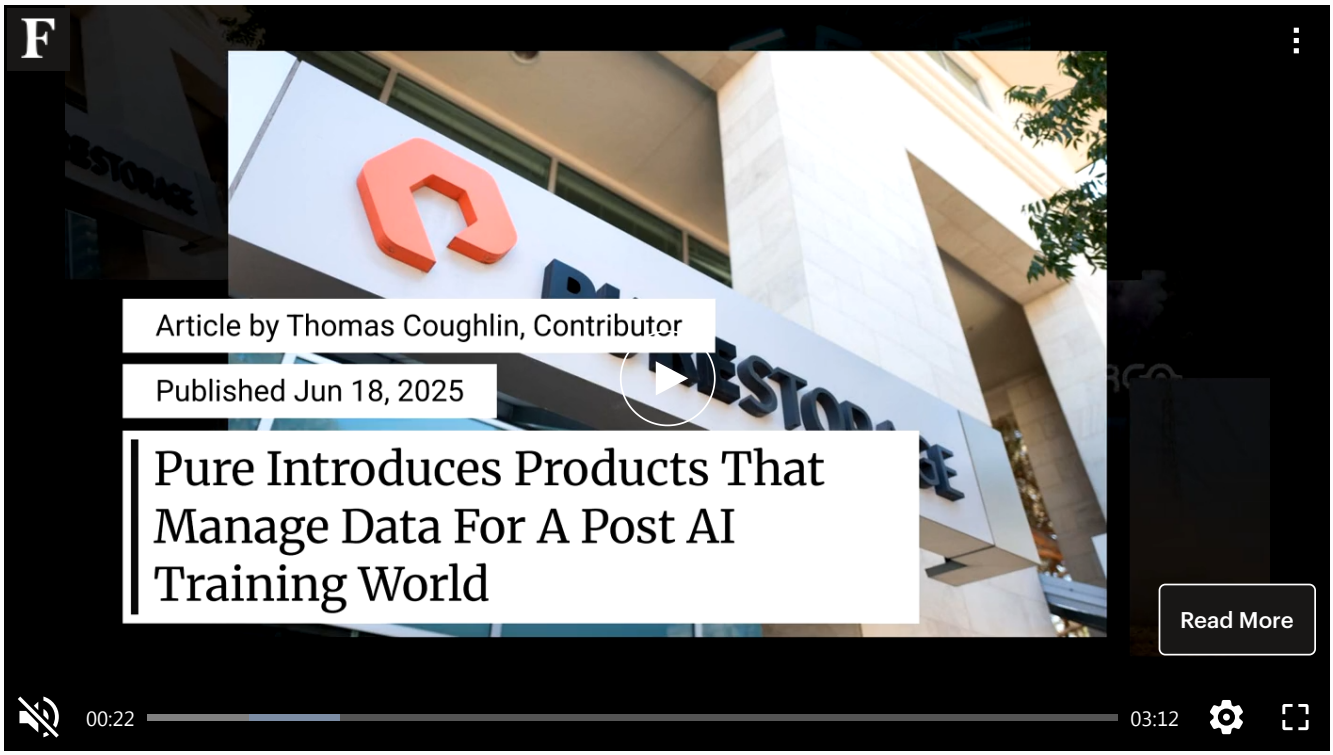
According to Vilius Petkauskas at Cybernews, whose researchers have been investigating the leakage since the start of the year, "30 exposed datasets containing from tens of millions to over 3.5 billion records each," have been discovered. In total, Petkauskas has confirmed, the number of compromised records has now hit 16 billion. Let that sink in for a bit. These collections of login credentials, these databases stuffed full of compromised passwords, comprise what is thought to be the largest such leak in history.

The 16 billion strong leak, housed in a number ion supermassive datasets, includes billions of login credentials from social media, VPNs, developer portals and user accounts for all the major vendors.

Remarkably, I am told that none of these datasets have been reported as leaked previously, this is all new data. Well, almost none: the 184 million password database I mentioned at the start of the article is the only exception.

“This is not just a leak – it’s a blueprint for mass exploitation,” the researchers said. And they are right. These credentials are ground zero for phishing attacks and account takeover. “These aren’t just old breaches being recycled,” they warned, “this is fresh, weaponizable intelligence at scale.”

Most of that intelligence was structured in the format of a URL, followed by login details and a password. The information contained, the researchers stated, open the door to “pretty much any online service imaginable, from Apple, Facebook, and Google, to GitHub, Telegram, and various government services.”



Strong Password Management Is Essential In Light Of Mega-Leaks Such As This One

Not all password databases are tye result of compromise and infostealer malware, such as is the case with the 16 billion megadump here. Darren Guccione, the CEO and co-founder of Keeper Security, a privileged access management platform, told me that this GOAT passwords leak was an apt reminder of "just how easy it is for sensitive data to be unintentionally exposed online." And Guccione certainly isn't wrong, far from it in fact. This could be just the tip of the biggest security iceberg waiting to crash into the online world. I mean, just imagine how many exposed credentials, including passwords, are sitting there in the cloud, or more to the point in misconfigured cloud environments, waiting for some to find them. If we are lucky, that someone will be a security researcher who responsibly discloses the exposure to the owner or host; if not, then it will be a malicious actor. Who would you put your money on?

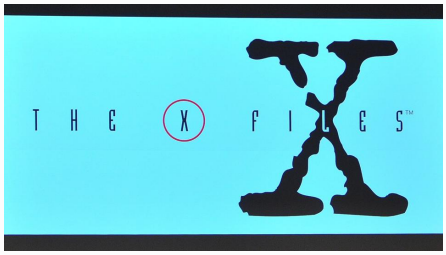
"The fact that the credentials in question are of high value for widely used services carries with it far-reaching implications," Guccione said, which is why it is more important than ever for consumers to invest in password management solutions and dark web monitoring tools. The latter can help by alerting users when their passwords have been exposed online, hopefully enabling them to take direct action and update their account logins if the password has been reused across services.

adopting zero-trust security models that provide privileged access controls to "limit risk by ensuring access to sensitive systems is always authenticated, authorized and logged," Guccione concluded, "regardless of where the data lives."

FORBES

Windows XFiles Attack — Your Passwords Are In Danger

By **Davey Winder**

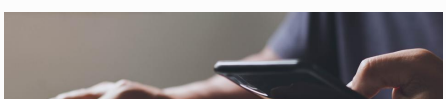


Cybersecurity Is A Shared Responsibility – Don't Share Your Passwords

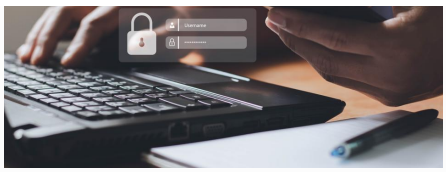
Ultimately, this reinforces that cybersecurity is not just a technical challenge but a shared responsibility. "Organisations need to do their part in protecting users," Javvad Malik, lead security awareness advocate at KnowBe4, said, "and people need to remain vigilant and mindful of any attempts to steal login credentials. Choose strong and unique passwords, and implement multi factor authentication wherever possible."

To which I would add: change your account passwords, use a password manager and switch to passkeys wherever possible. Now is the time to take this seriously, don't wait until your passwords show up in these ongoing leak datasets – get on top of your password security right now.

FORBES



Microsoft Account Password Spraying Attack Confirmed — Act Now



By **Davey Winder**

Editorial Standards | Reprints & Permissions

Find Davey Winder on LinkedIn and X. Visit Davey's website. Browse additional work.

Follow Author

Join The Conversation

Comments 0

One Community. Many Voices. Create a free account to share your thoughts. Read our community guidelines here.

See All Comments (0)

Forbes