The Washington Post
Democracy Dies in Darkness

Worried about the 23andMe hack? Here's what you can do.

A bad actor offered to sell information on 23andMe's users, calling out Jewish people specifically

By Tatum Hunter

Updated October 12, 2023 at 3:24 p.m. EDT | Published October 12, 2023 at 7:00 a.m. EDT

Fourteen million people have shared their genetic information with 23andMe in hopes of learning more about their heritage. After a hack that appeared to target people with Jewish ancestry, some might be wondering how to cut ties with the company.

The apparent hacker posted in an online forum last week offering to sell the names, locations and ethnicities of what could be millions of 23andMe users, calling out Jewish people specifically. 23andMe confirmed to The Washington Post that the leak contained real data and said the hack appeared to be the result of credential stuffing, in which an attacker uses leaked username-password combinations from other sites to break into 23andMe accounts. (Imagine you used the same password for 10 websites, then one of those sites had a security breach.)

It's not the first time 23andMe has come under fire for data privacy and security concerns. After local police used a DNA database in 2018 to arrest a man believed to be a serial killer, genetic-testing companies including Ancestry and 23andMe promised to start disclosing law enforcement requests and obtaining customers' "separate express consent" before handing over information about their genetics to outside companies, including insurance agencies. (23andMe, for its part, was already disclosing law enforcement data requests at the time. A spokesman said it doesn't share information directly with insurance agencies.)

The type of information genetic-testing companies collect is currently not protected by the Health Insurance Portability and Accountability Act (HIPAA), our nation's health privacy law. 23andMe still allows for third-party data sharing in its privacy policy.

23andMe said in a blog post that hackers probably broke into individual accounts and used the site's "DNA Relatives" feature to compile lists of people. After noticing the incident, the company enlisted the help of digital forensics experts and law enforcement, it said. 23andMe is requiring all users to reset their passwords.

If you're concerned about the leak, there are a few things you can do to keep yourself safe.

Choose unique, impossible-to-guess passwords

All 23andMe users should promptly reset their passwords to something they've never used on other sites.

If you can remember your password off the top of your head, it's not strong enough, said Boyd Clewis, CEO of

If you can remember your password off the top of your head, it's not strong enough, said Boyd Clewis, CEO of cybersecurity company Baxter Clewis. Choose a unique password, he said, and make it complicated enough that no one could piece it together. You can rely on a password manager such as Dashlane or 1 Password to save your passwords and insert them automatically when you log in.

Request to delete your data

You can ask 23andMe and other genetic testing companies to delete the information they're storing on you. If you live in a state with a comprehensive privacy law, such as California, Virginia or Colorado, the company is required to do so.

If you're a 23andMe customer, you can request your information be deleted from inside your account settings. The company will email you for confirmation, after which it will permanently delete your account, stop using your data in new research studies and destroy your genetic sample if you gave permission to store it.

A 23andMe spokesman said the company retains some data because of legal and lab requirements. He declined to say whether that includes individual genetic information.

If you haven't already, think twice before sharing genetic information

Sharing your genetics with a DNA database puts you at greater risk of botched criminal procedure, discrimination from insurance companies and employers, and targeted attacks such as blackmail, privacy experts say.

23andMe said it didn't find any evidence of a "data security incident" in last week's leak, a distinction it drew because the information hackers gathered was available to opted-in users. But putting the burden on consumers to protect their own sensitive data with strong passwords and careful management is wrongheaded, said Suzanne Bernstein, a law fellow at digital rights nonprofit Electronic Privacy Information Center.

"If 23andMe is collecting, storing and processing a tremendous amount of very highly sensitive personal data, I think at the end of the day they should take responsibility for that," she said.

The solution, according to Bernstein, is not to expect consumers to evaluate each company by sifting through long and hard-to-understand privacy policies — but for lawmakers to pass and enforce tough privacy and security rules that companies can't wriggle around.