Genetic testing firm 23andMe admits hackers accessed DNA data of 7m users

Publication Date: 2023-12-05

Author: Edward Helmore

Section: Technology

Tags: Hacking, news

Article URL: https://www.theguardian.com/technology/2023/dec/05/23andme-hack-data-breach

The genetic testing company 23andMe has said that nearly 7 million people have been affected by a security breach that put DNA ancestry information into the hands of hackers who broke into the site in early October. On Friday, the California-based company said in a regulatory filing that the personal data of 0.1% of customers – or about 14,000 individuals – had been accessed by "threat actors". But the filing warned that hackers were also able to access "a significant number of files containing profile information about other users' ancestry". The company confirmed to TechCrunch on Saturday that because of an opt-in feature that allows DNA-related relatives to contact each other, the true number of people exposed was 6.9 million – or just less than half of 23andMe's 14 million reported customers. Another group of about 1.4 million people who opted in to 23andMe's DNA relatives feature also "had their family tree profile information accessed", the company also acknowledged. That information includes names, relationship labels, birth year, self-reported location and other data. 23andMe said in a statement: "We were made aware that certain 23andMe customer profile information was compiled through access to individual 23andMe.com accounts. "We believe that the threat actor may have then, in violation of our terms of service, accessed 23andme.com accounts without authorization and obtained information from those accounts." Two months ago, Wired reported that a sample of data points from 23andMe accounts were exposed on BreachForums, a black-hat hacking crime forum. The hackers claimed the sample contained 1m data points exclusively about Ashkenazi Jews. According to the outlet, there also seemed to be hundreds of thousands of users of Chinese heritage affected by the leak. Hackers then began selling 23andMe profiles for between $1 and $10 per account, with information revealed that included some details about genetic ancestry results, like "broadly European" or "broadly Arabian". Later, hackers released 23andMe user information containing records of 4 million users. The hackers claimed the information included people from the UK with some of the "the wealthiest people living in the US and western Europe on this list". TechCrunch said it had analysed the leaked data and determined that some records matched genetic data published online by hobbyists and genealogists. But the outlet also suggested the hacked data was at least in part from 23andMe. When the company first disclosed the breach, it said it was likely that it was caused by customers reusing passwords that have already appeared in other data breaches, allowing hackers to use a technique known as "credential stuffing". "It just comes down to the fact that humans reuse their passwords – that's what makes it possible," Ronnie Tokazowski, a longtime digital scams researcher, told Wired. "And the fact that it's claiming to target a Jewish population or celebrities – it's not shocking. It reflects the underbelly of the internet."