Click “Download PDF” above to activate the article’s links.

23andMe personal data exposure

Bro. Hal Bookbinder

On October 6, 2023, 23andMe announced, “We recently learned that certain 23andMe customer profile information that they opted into sharing through our **DNA Relatives feature**, was compiled from individual 23andMe.com accounts without the account users’ authorization.” Read more here.

On October 9, 2023, they issued an update noting that their investigation continues and, “We are reaching out to our customers to provide an update on the investigation and to encourage them to take additional actions to keep their account and password secure. Out of caution, we are requiring that all customers reset their passwords and are encouraging the use of multi-factor authentication (MFA).”

The announcement did not share specifically what data was compromised, or that this data is now available for sale on the dark web. Possibly, a further update from 23andMe by the time you read this will include this. The updates thus far have neither been forthcoming, nor complete. The tone of the updates seems to shift blame to the user, rather than taking any corporate responsibility.

According to Bill Toulas at *bleepingcomputer.com*, “Late last month, a threat actor leaked 23andMe customer data in a CSV file named 'Ashkenazi DNA Data of Celebrities.csv' on hacker forums. The file allegedly contained the data of nearly 1 million Ashkenazi Jews who used 23andMe services to find their ancestry info, genetic predispositions, and more.” Read more here.

The threat actor apparently obtained passwords that were exposed on other sites and reused on 23andMe. They were then able to retrieve publicly available personal information that users share to facilitate links, including full name, year of birth, city and state, and ancestry information. I have 1,504 DNA “relatives” in 23andMe and so if any of them were hacked, my public information could be seen.

My password on 23andMe is long, complex, and unique. However, this does not protect me from exposure of my publicly available information as others among my 1,504 “relatives” likely reuse passwords and may have been hacked elsewhere. While I considered hiding my public information, or even turning off the DNA Relatives feature, in the end I decided against this.

The publicly facing information in 23andMe is easily found elsewhere on the web. Look yourself up in https://www.fastpeoplesearch.com/ and you will likely find your name, contact information, even month and year of birth. However, I am disappointed with 23andMe for its lack of internal mechanisms to catch such mass extraction of data, and for its lack of transparency.

In the end, we may learn that the issue with 23andMe goes deeper than the reuse of passwords. At this point, it is too early to speculate. This situation does highlight, however, the need for each of us to use unique, complex passwords for each site that we access, to employ MFA, and to be conscious of the information we share publicly, recognizing that once it is out there, where it will end up is anybody’s guess.

As can be expected in our litigious society, several class-action lawsuits have already been filed against 23andMe. Read more here.

Bro. Bookbinder is a retired Information technology director and university instructor. This is the 96th article in this series. All articles can be accessed at https://tinyurl.com/SafeComputingArticles.