SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
**E:** sales@sonmax.com
**T:** +1 732.591.1512
**F:** +1 732.591.5424
www.sonmax.com

# Notice of data breach


On June 14th I received an urgent message from MyHeritage, one of the nation's largest genealogy sites. It had a subject "Important: Account security alert and instructions for securing your account". On opening the mail, the header said "Notice of data breach" and the body of the letter detailed their version of what happened, what they are doing to address the problem and what I should do in response.

My initial thought was that they seemed to be following a well-defined process in a timely fashion. And then I actually read the note closely.

To my dismay, 92.3 million clients were impacted. Worse, the dwell time associated with the breach (i.e., the time from the breach to the discovery of the breach) was 221 days. Worst, MyHeritage **NEVER** discovered the breach. The breach was only discovered when MyHeritage's CISO received a message from a security researcher, which stated that the researcher had found a file named "myheritage" containing email addresses and hashed passwords.

Upon receiving this message, MyHeritage reviewed a copy of the file and confirmed its authenticity. They then purportedly issued a public announcement on the evening of June 4th. The problem with their announcement was that it appeared only as a blog on their website and was not a global PR release.

They went on to detail all of what they are doing to address the problem:

- They immediately set up an incident response team to investigate the incident
- They engaged a leading (their word) independent cybersecurity firm to conduct comprehensive forensic reviews; conduct an assessment and recommend steps to prevent future such incidents
- They notified relevant authorities per GDPR

- They set up a 24/7 customer support team to assist with customer questions
- They expired all existing passwords on MyHeritage
- They added two-factor authentication as an option to their site
- They urged customers to change their password on any other site that may have had the password that was used on MyHeritage

As I reviewed the above, I started asking the following questions:

1) Why would a business, with 92.3 million clients not already have a tested and robust incident response plan with a standing incident response team in place? Why are they just setting one up now?
2) They claimed to have engaged a leading cybersecurity firm; but they won't and didn't say who the firm was? What is the basis of their claim that it's a leader in the incident response space? Is it a firm such as Kroll, Mandiant or Stroz Friedberg? If so, say so.
3) They notified authorities per GDPR? Which authorities and when? Did EU-based clients have their right to be forgotten being followed?
4) They urged customers to change their password on any site that used the same password as the one on MyHeritage. Why? They claim that the exfiltrated data only contained hash information. If one enters the hashed information in the password field, the logon would have to fail…unless there's an additional security flaw in their logon process.
5) They claim that ONLY email addresses and hashed password records were exfiltrated. How do they know that if the "leading cybersecurity" firm has not finished their forensic review? And after 11 days, they haven't!

In other words, MyHeritage no clue as to the level of damage done by the data breach. They don't know the scope of the damage. They claim that credit card data was not impacted, but they have no verifiable third-party proof to support that contention.

My conclusion is that if you are/were a MyHeritage customer, your data is at risk. We all have an affirmative obligation to monitor all of our personal data in any venue and keep it safe. Now we wait for the forensic review to complete to see how much actual damage was done.

Stay safe out there.

***Knowledge and awareness are your best defense!***
***Please follow me on twitter: @stevewertheim***