The MyHeritage Data Breach and How We Should Strategize

Alexei Hooks, anh5653@psu.edu

Over the past few days, the company, MyHeritage, has been notified of a breach that has an unknown origin date could have affected 92 million of their customers. The company has reported that a file containing customer’s emails and encrypted passwords on a server that was not managed by their staff (Mole). This breach could spell disaster for the reputation of MyHeritage among their customers, as the integrity of their security could be negatively affected. As information has come out about the breach, the company has made customers aware of the fact that personal emails have been stolen. Along with this, MyHeritage is asking their customers to change their password as this would mitigate the chance of future information from their accounts from being illegally taken.

This breach may call for our company to upgrade and regroup from a security standpoint. As the breach was against a company with a similar structure and function, we need to double down on security. Other potential threat actors may have seen the recent news about the MyHeritage breach, and are now trying to find ways into systems of similar companies. Attacks can come in many forms, so possibly bringing in extra teams of security specialists for the next few weeks would be advisable. According to Oleksandr Maidaniuk of the DigitalGuardian.com, the best way to deal with a breach in the industry is to be direct with the customers, mitigate potential threats, and educate the rest of the industry on how to prevent an attack such as the MyHeritage breach from happening again (Digital Guardian). The mitigation process may be hard as we, as a company, have not been breached, but making sure our employees and customers are acting safely with links needs to be reinforced. Any action our business does moving forward for the foreseeable future needs to have security in mind, as a breach in just a click away.

The best thing to do in a time such as this is to have clear communication that our customer’s information is the most important part of our business. When assessing our next step, we should be sure to make them public, as this could strengthen our relationship with our valued customers. Especially with the use of DNA and testing of it, this security should not be taken lightly. Personal information could be used in variety of malicious ways, and we need to make sure that customers know we are on their side. This could include social media announcements, a speech from the CEO to be posted on our website, or any other form that the marketing team can come up with in order to connect with our customers.

With the breach of a similar company, we need to defend our systems, assess any potential risks, and communicate with our customers what and how we are using their data. These actions, if completed thoroughly, should be the best way to properly secure and maintain our customers and their data.

References

"92 Million User Accounts at Risk after Genealogy and DNA-Testing Site Myheritage Is Hacked." *BetaNews*, 6 June 2018, https://betanews.com/2018/06/06/myheritage-hacked/.

Beth Mole - Jun 5, 2018 10:38 pm UTC. "92 Million Myheritage Users Had Their Data Quietly Swiped." *Ars Technica*, 5 June 2018, https://arstechnica.com/tech-policy/2018/06/92-million-myheritage-users-had-their-data-quietly-swiped/.

"Data Breach Experts Share the Most Important next Step You Should Take after a Data Breach in 2019 & Beyond." *Digital Guardian*, 11 Aug. 2020, https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015.

Golightly, Daniel, et al. "PSA: Myheritage Breach Leaks 92 Million User Emails." *Android Headlines*, 5 June 2018, https://www.androidheadlines.com/2018/06/psa-myheritage-breach-leaks-92-million-user-emails.html.