Genetic Data Under Attack: 23andMe Cybersecurity Breach & What Comes Next?

Abigail Downs

In October 2023, 23andMe experienced a significant cybersecurity breach, impacting nearly seven million individuals who had utilized their genetic testing platform. Despite initial speculation that the breach might be linked to vulnerabilities in 23andMe's cyber infrastructure, investigations revealed that the intrusion was external. The breach occurred when malicious hackers successfully hacked user accounts by stealing recycled passwords from other websites. These hackers then exploited the platform's social features to access sensitive genetic information from other users. The compromised data included various personal details such as names, birthdates, information about relatives, and, most critically, sensitive data related to DNA profiles.

The alarming cyberbreach resulted in the exposure of customer information from individuals of Ashkenazi Jewish ancestry, Chinese ancestry, and British ancestry, respectively, on the dark web. Genetic data plays a pivotal role in propelling healthcare research, facilitating clinical testing, and enhancing disease prevention. However, it also introduces a significant risk by exposing individuals' most fundamental vulnerabilities in their purest form: through their DNA.

The 23andMe breach highlights the need for heightened cybersecurity measures and policies across online platforms. Recently, 23andMe asserted that they attribute the security breach to customer negligence, citing the reuse of passwords. However, it is important to note that not all compromised DNA profile information originated from the breached accounts, as some victims were linked through the platform's social features.

This breach highlights the constant challenges in safeguarding sensitive genetic and personal information in the digital age. In response to the breach, 23andMe has taken proactive steps, including implementing enhanced security protocols and measures to strengthen its systems and safeguard the privacy of its users. Nevertheless, these efforts alone are not sufficient.

The United States currently lacks robust cybersecurity policies for companies handling highly sensitive data. Strengthening and enforcing comprehensive cybersecurity regulations is essential to preventing these types of breaches from happening again. In the case of individual businesses, like 23andMe, this entails implementing safeguards that prevent hackers from exploiting social features to compromise other accounts or mandating customers to respond to security questions before accessing their accounts. For US policy, this involves the implementation of stricter regulations regarding the storage and location of sensitive data and restricting access to that information within these companies. Additionally, there is a long-term need to protect customers of companies holding sensitive data from acquisition scenarios where the information may no longer be adequately protected.

In the meantime, one ought to be leery of the companies and platforms trusted with private information. No company is immune to breaches. Recommendations to mitigate such risk include changing passwords on a quarterly basis, avoiding password reuse across different accounts, taking proactive measures such as enabling two-factor authentication, setting up identity monitoring, and implementing other available safety protocols. Consistently staying vigilant and prioritizing cybersecurity practices will contribute to a safer online experience, and hopefully prevent a breach like 23andMe's from happening again.

For more information, check out the full article here.