

John Heath

10/11/2025

Sharing genetic information on the internet has some very serious implications. Organizations such as *23andMe* and *Ancestry* utilize genetic information to provide information on an individual's ancestry. Their services are becoming increasingly more popular, with more people growing curious about their family lineage. Despite the seemingly harmless service that these organizations provide, they can include some rather serious security implications. In basic cybersecurity, the average individual is concerned with things like banking information or text message privacy. In biocybersecurity, individuals are concerned with the privacy of their genetic makeup. While both are extremely important, there is one key difference that highlights the importance of biocybersecurity. If someone gains access to your credit card, you can freeze it and get a new one. If someone gains access to your genetic information, there's no changing it. The attacker would have access to your genetic information forever. From there, this information could be sold to insurance companies, then used against you. Insurance companies could specifically avoid the business of those who suffer from certain genetic disorders or diseases. Additionally, hackers could utilize genetic data to enhance their ability to commit phishing attacks. In phishing attacks, the attacker must gain some sort of credibility in the email to get the recipient to click the link to the malware. For example, a phishing email could contain private genetic information about the victim of the attack, with the attacker claiming to be the individual's doctor or local hospital. This would build credibility, ultimately enhancing the attacker's ability to access private information.