Write Up: Hacking Humans

This article did a great job at raising serious cybersecurity and ethical concerns about digitizing human DNA. As a cybersecurity major, what stood out to me the most is how our genetic data is now becoming easily accessible information that can be hacked, stolen, and exploited. Companies offering DNA testing that can be mailed to your home and done with a simple cheek swab have made it easy for people to share their genetic code online. Not many of these people understand the risks of uploading this private and identifiable information.

The author, Rizkallah, says that DNA is the "ultimate identifiable information" because it cannot be altered or replaced if stolen or compromised in any way. This introduces a new domain called cyberbiosecurity. This domain primarily focuses on protecting digital biological data from security threats and cyber attacks. The potential consequences of a DNA breach go far beyond traditional cyber theft. Criminals could sell our genetic data for profit, or even use it for malicious purposes such as biological manipulation.

What I found most interesting is that "hacking humans" has evolved from phishing emails and ransomware to now going after very personal and identifiable data like DNA. Cybersecurity professionals must take this emerging threat seriously by implementing stronger encryption and access controls in biotech systems. As future defenders in this field, we need to be aware that protecting personal data now includes protecting the code that makes us who we are. If we fail to secure it, we risk the most personal kind of identity theft imaginable—our genetic identity.