Name: Huong Quach

Date: 06/08/25

Hacking Humans

BLUF

Since DNA is the most sensitive and permanent type of personal data, digitizing human DNA through consumer testing services presents serious privacy and security threats. Although this kind of digitization has advantages for science, it also makes it more vulnerable to abuse, identity theft, and cyberattacks.

Summary

Given that human DNA is the most sensitive and permanent type of personal data, digitizing it for consumer testing services presents serious privacy and security problems. Despite the scientific advantages of such digitization, it also makes it more vulnerable to abuse, identity theft, and cyberattacks. It is critically necessary to increase consumer awareness and strengthen security measures to keep this important data safe from attackers.

The growing topic of cyberbiosecurity, which examines the relationship between biology and cybersecurity, includes DNA digitization. The essay highlights that although digital DNA offers enormous promise for improvement in science and medicine, hackers can profit greatly from it as well. Important security and ethical concerns are brought up by the potential for

hackers to access DNA databases. A stolen DNA profile may have more serious, long-term repercussions than a stolen Social Security number.

Future issues like the possible abuse of genetic information in hiring or law enforcement are also covered in the article. These risks are real, as evidenced by actual events, like as hacks that impact millions of people. Even if it hasn't happened much before, the risk of making money off of stolen DNA is growing as technology develops.

Ultimately, Rizkallah calls for heightened consumer awareness and stronger accountability from companies handling DNA data. She urges individuals to understand how their genetic information is stored, protected, and used, especially as society becomes desensitized to data breaches. The author asserts that innovation must be met with equal investment in security, warning that failure to protect DNA data could result in the most severe form of identity theft imaginable.

This article serves as a wake-up call to consumers, tech companies, and policymakers to recognize DNA as the most sensitive form of personal data and to take proactive steps to defend it against cyber threats.