Hacking Humans

Kevin A. Loarca

Old Dominion University

CYSE 200T: Cybersecurity, Technology & Society

Professor Christopher Bowman

June 14, 2026

The Ethics of Curiosity

The personal and medical benefits of DNA digitization outweigh the lifelong security risks. As stated in the article, the digitization of human DNA, for the purpose of science and medical research, could bear great fruit in curing fatal illnesses (Rizkallah, 2018). This perspective on DNA digitization is worth the potential security risks, as it is used to benefit society. However, the security risk should not be ignored while technology is used in combination with these types of scientific advancements. That said, there should be an additional focus on access and security when it comes to protecting this type of confidential information.

Corporate and Employment Privacy

The focus on access is important regarding the author's concern about "drawing the line" in privacy and the example they provide. The organizations conducting these scientific advancements need to protect information and avoid instances that could violate privacy. Otherwise, it could lead to misuses beyond their original intent, such as the example the author provides. Access to these databases by unauthorized parties could lead to issues of genetic discrimination in the workplace. For example, an employer could review the genetic makeup of two interviewees and select the one who doesn't pose future health problems that would affect their ability to work. The employer would discriminate against the other person as they create this negative assumption about their health.

The “Hacking Humans” Concept

As biological data becomes digitized, it creates an important need for security to be held and invested in. The presence of permanent biological data changes the view on “human factor” security compared to traditional digital passwords. There is no way to change the biological material, so when there is a possibility of a breach, the information is stolen permanently. Even if the systems were to have the best security, the risk is present from the people themselves. There are social engineering tactics that malicious actors can use to try to compromise those systems. This becomes far more dangerous if those within the organization are not taught the necessary security measures to prevent that type of attack.

Conclusion

The benefits of DNA digitization outweigh the lifelong security risks if it is to benefit society, such as science and medical research to cure illnesses. However, other additional factors need to be taken into consideration, such as access and security. Otherwise, it could lead to problems down the line. The misuse of the data collected could be used far from its intended purpose and allow discrimination in a workplace if the data does not remain private. Additionally, there is the security concern that biological data has, as it is permanently identifiable information. This changes the view on the human factor of security as it poses a dangerous and heavy consequence if they are not taught the necessary security measures.

References

Rizkallah, J. (2018, November 11). *Hacking Humans: Protecting Our DNA From Cybercriminals*. Perusall. https://app.perusall.com/courses/202530_cyse200t_33004-cybersecurity-technol-society/hacking-humans_-protecting-our-dna-from-cybercriminals?assignmentId=2hiDxZ3Qp66dMSHJe&part=1&filter=all