Destiny Hale

3/30/25

Hacking Humans

Human hacking is one of the most common cyber attacks in the world. By understanding and studying human behavior, hackers can manipulate the minds of users and gain personal information from the users' mistakes or human errors. However, this human hacking involves gaining DNA information of individuals used for personal gain by attackers. Digital DNA services are a recent innovation in the digital age; however, numerous challenges and impacts from this innovation may put individuals in harm's way. In this write-up, I'll discuss DNA privacy challenges and its impacts, the exploitation of genetic information, emerging DNA cybercrimes, and mitigation solutions to combat these cyberattacks.

Privacy Challenges and Impacts

The nature of DNA is a valuable part of our human nature. This biological structure includes several generations of genes from our ancestors and numerous proteins. What makes this structure unique is that although we have the same sequence, we are made different through several variations. DNA creates our person and identity as a whole. Out of curiosity, numerous people use their DNA to find out about their past, ethnicity, nationality, and extended relatives outside the immediate. However, in recent years, cyber attacks regarding DNA leaks led to the violation of privacy of numerous individuals. Rizkallah (2018) questioned whether the digitalization of our DNA is the safe way to go. In the "Hacking Humans" article, she stated that if we look at our DNA as personally identifying information or PII, hackers can still use this as a

benefit for personal gain from sales on the black market and great access to DNA service websites. She also stated that our DNA is permanent and irreplaceable compared to our social security numbers which also define our identity. This raises concerns about privacy because this increases the motive for hackers to target DNA databases and services.

Arshad et al. (2021) highlight the security and privacy challenges in direct-to-customer (DTC) companies and DNA databases through an analysis. Direct-to-customers (DTC) companies such as 23AndMe, Ancestry.com, and GEDMatch collect a large amount of genetic information. They also share this information with third parties for research purposes without the individual's consent (Arshad et al., 2021). Informed consent plays a role in everything, it involves granting permission from the individual to opt-out or proceed and to disclose any personal information with the service. Without transparency and control over their DNA, this leads to long-term privacy breaches and misuse of genetic information.

In the analysis, Arshad et al. (2021) found numerous vulnerabilities within open-source DNA database systems. A couple of vulnerabilities they have discovered are unsafe functions, lack of authentication, publicity of genetic data, and use of HTTP, not HTTPS. Within the code of the system, they have found functions such as ‘gets’, ‘scanf’, ‘strlen’, etc. which these commands can lead to a buffer overflow. In these databases are stored valuable information; however, with no access controls or authentication, the integrity and confidentiality can be compromised. For the individual, this is a violation of autonomy due to the exposure of their DNA information.

Most of the genetic information is publicly available through online databases; however, the risks of this being exposed can lead to hackers leaking personally identifiable information via identifying hidden patterns within the data (Arshad et al., 2021). HTTPS or Secure Hypertext Transfer Protocol is a protocol that encrypts the communication between web servers and websites.

However, in some DNA platforms or databases, they only contain HTTP which is weak and vulnerable to attacks such as man-in-the-middle (Arshad et al., 2021). The impacts of these vulnerabilities could discourage customers from using these services for the protection of their privacy.

From a legal perspective, most genetic tests aren't regulated due to companies selling them without independent verification of the seller's claims (National Human Genome Research Institute). However, the FDA, FTC, and CMS regulate these based on three criterias: analytical validity, clinical validity, and clinical utility. Analytical validity tests the accuracy of prediction about the presence or absence of a genetic change. Clinical validity tests the analysis of genetic variants related to the presence, absence, or risk of a specific disease. Lastly, clinical utility refers to how accurately the test can provide information to patients regarding treatments, diagnoses, management, etc (National Human Genome Research Institute). Both the FDA and CMS regulate analytical validity and clinical validity to expand policies and oversight. As for clinical utility, frameworks are currently being developed.

Exploitation of Genetic Information

The accessibility of open-source DNA databases and services not only amplifies privacy and security concerns, but also opens opportunities for possible exploitation of genetic information, involving genetic discrimination, identity theft, and law enforcement profiling. Genetic discrimination is when people are treated differently by their employer or insurance company because the individual has a genetic mutation that increases the inherited disorder (U.S. National Library of Medicine, 2021). Employees may be denied commerce or progression openings based on their conditions (Vavekanand, 2024). In insurance companies, they may deny or

charge higher premiums to the individual based on their atypical genetic makeup. From a social perspective, the individual may face social disgrace and isolation (Vavekanand, 2024).

Identity theft is a standard cyber attack involving stealing another person's identity. Most of these attacks involve malicious actors using social security numbers or any other information that is used to identify a person to impersonate the individual. In this case, with the use of genetic information, malicious actors can influence individuals to share personal information or pay for fake testing or treatment services (Vavekanand, 2024). They can also use this to retrieve electronic health records or other sensitive information. Therefore, DNA identity theft causes irreversible harm to the individual.

In criminal investigations, law enforcement uses DNA to track a criminal down for a crime they committed. However, there have been cases of law enforcement using Direct-to-customer (DTC) DNA services to find criminals they haven't caught and possible suspects. GEDMatch is an open-source site that allows you to upload raw DNA files (Lo, 2024). This service analyses the results and produces a list of family relatives who have opted into its service (Lo, 2024). In addition, this also lists the contact names, death certificates, and birth certificates for a better family tree connection. Law enforcement found that this was a helpful tool in finding potential suspects and criminals they hadn't found. Using the list of family members helps narrow down the search. Once they obtained the information, they put this into their database. This brings up whether law enforcement has violated terms and service and the fourth amendment.

Emerging DNA Cybercrimes

According to Rizkallah (2018), hacking humans will continue. Numerous cybercrimes have centered around social engineering and phishing attacks. Social engineering and phishing involve

manipulating the target into giving their personal information and using it for personal gain. As for DNA, malicious actors can use this genetic information to create bio-malware and attack DNA databases to cause data breaches. Bio malware refers to the use of biological agents or synthetic DNA in malware (Dawes Centre for Future at UCL, 2021). Criminals can obtain information by gaining access to competitors' systems through biological malware (Dawes Centre for Future at UCL, 2021).

Numerous DNA databases often lack robust security which creates an opportunity for hackers to exploit these systems and cause data breaches. For example, in October 2023, 23AndMe was a victim of a data breach by a cybercriminal named Golem (Holthouse et al., 2025). Over 4 million users' information has been exposed on a hacker forum called BreachForums. Within the 23AndMe database were a few vulnerabilities such as the DNA relatives feature, weak passwords, and API security failures. The DNA relatives is a feature that helps users to identify and connect with other relatives. This also allows them to see shared genetic markers, estimated relationships, and other personal information (Holthouse et al., 2025). However, the risk is if an attacker gains hold of this feature, they will be able to obtain data from numerous profiles. From this risk, the hacker was able to gain access through the network and exposed over 5.5 million DNA relative profiles and 1.4 million Family Tree profiles.

Weak passwords are a common security flaw within systems and databases. In the 23AndMe dataset was over 300,000 Chinese compromised passwords; the most common was ‘123456’ (Holthouse et al., 2025). In their authentication infrastructure were weak login APIs and a lack of rate limits. The hacker was able to make an unrestricted number of login attempts. From these vulnerabilities, the hacker was able to attack with brute force and credential stuffing.

Through these data breaches, hackers can steal genetic credentials and sell them on black markets or blackmail individuals.

Mitigation Solutions

Although we can't entirely stop these DNA privacy concerns, exploitation, and cybercrimes, we can slow them down by using mitigation techniques such as public awareness, encryption, and access controls. According to Andrews et al. (1994), an informed public is the best protection from potential abuse of genetic technology and information. In addition, this also allows them to make informed decisions about whether they want to continue participating in services or opt-out for privacy reasons. Another way the public can stay informed is through research and asking questions. This helps them to be familiar with genetic technology and cybersecurity practices to keep their genetic data safe.

To strengthen the security posture of DNA services, using access controls and cryptography can prevent the data from being exposed and breached. An access control such as multi-factor authentication can be implemented for all users, preventing the compromise of their accounts (Holthouse et al., 2025). Implementing access control schemes and policies can improve genomic privacy (Arshad et al., 2021). Most of the genetic information on these services isn't fully protected which raises the accessibility to hackers. The use of strong cryptographic measures can be adopted and encouraged within these domains (Arshad et al., 2021).

Conclusion

Digital DNA services are a recent innovation in today's time and are often used to discover other family members. However, this innovation puts individuals in harm such as the violation of privacy, exploitation of genetic information, and the emergence of DNA cybercrimes. Direct-to-customers and open-source DNA services raise privacy and security concerns due to the lack of transparency and vulnerabilities found in their system. The impacts of both violate autonomy and discourage users from using their services for the protection of their privacy. However, numerous regulations are being made to further protect their privacy. The accessibility of these services opens opportunities for genetic exploitations such as genetic discrimination, identity theft, and law enforcement profiling; causing social exclusion, irreplaceable identity harm, and violations of privacy rights. In addition, they can also cause cyber crimes such as data breaches and bio malware attacks from their weak security systems. Although these concerns, exploitations, and crimes can't be stopped, they can be mitigated by public awareness, access controls, and cryptography for better cybersecurity practices and security posture.

References

Andrews, L. B., Fullarton, J. E., Holtzman, N. A., & Motulsky, A. G. (Eds.). (1994, January 1). *Public education in Genetics*. Assessing Genetic Risks: Implications for Health and Social Policy. https://www.ncbi.nlm.nih.gov/books/NBK236046/#ddd00155

Andrews, L. B., Fullarton, J. E., Holtzman, N. A., & Motulsky, A. G. (Eds.). (1994b, January 1). *Social, legal, and ethical implications of genetic testing*. Assessing Genetic Risks: Implications for Health and Social Policy. https://www.ncbi.nlm.nih.gov/books/NBK236044/

Arshad, S., Arshad, J., Khan, M. M., & Parkinson, S. (2021, May 20). *Analysis of security and privacy challenges for DNA-genomics applications and databases*. Journal of Biomedical Informatics. https://www.sciencedirect.com/science/article/pii/S1532046421001441#s0040

Holthouse, R., Owens, S., & Bhunia, S. (2025, February 6). *The 23andMe data breach: Analyzing credential stuffing attacks, security vulnerabilities, and Mitigation Strategies*. arXiv.org. http://www.arxiv.org/abs/2502.04303

Lo, K. (2024, April 29). *Whose DNA is it anyway? Legal Challenges That Arise from the Use of Genetic Genealogy in Criminal Investigations*. Richmond Journal of Law and Technology. https://jolt.richmond.edu/2024/04/26/whose-dna-is-it-anyway-legal-challenges-that-arise-from-the-use-of-genetic-genealogy-in-criminal-investigations/

National Human Genome Research Institute. (n.d.). *Regulation of genetic tests*. Genome.gov. https://www.genome.gov/about-genomics/policy-issues/Regulation-of-Genetic-Tests

Rizkallah, J. (2018, November 29). Hacking humans: Protecting our DNA from Cybercriminals. Forbes. https://www.forbes.com/councils/forbestechcouncil/2018/11/29/hacking-humans-protecting-our-dna-from-cybercriminals/

Synthetic Biology and future crime. Dawes Centre For Future Crime At UCL. (2021, November). https://www.ucl.ac.uk/future-crime/sites/future_crime/files/synthetic_biology_and_future_crime_final_021221.pdf

U.S. National Library of Medicine. (2021, July 28). What is genetic discrimination?: Medlineplus Genetics. MedlinePlus. https://medlineplus.gov/genetics/understanding/testing/discrimination/

Vavekanand, R. (2024). Data Security and Privacy in Genomics Research: A Comparative Analysis to Protect Confidentiality. Studies in Medical and Health Sciences, 1(1), 23–31. https://doi.org/10.48185/smhs.v1i1.1158