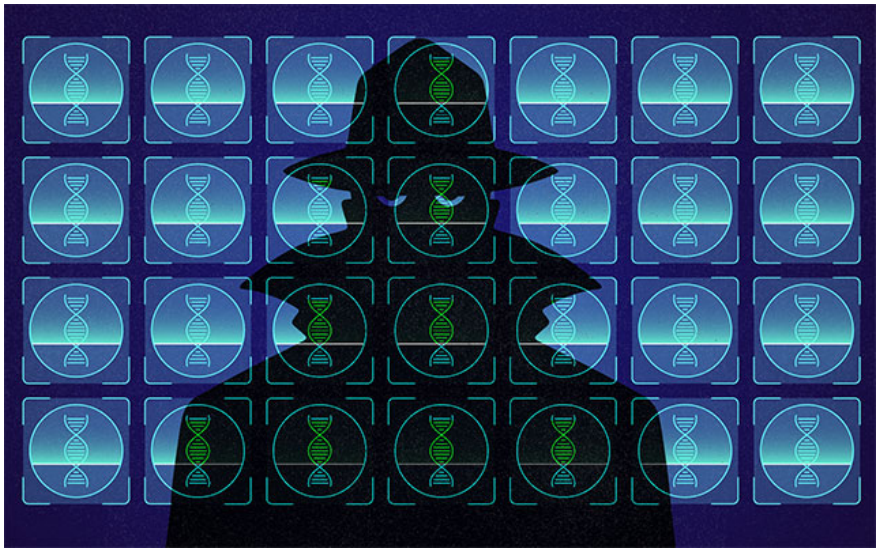
Warning: Your DNA data can be hacked and misused

Scientists warn that without improved security measures, hackers could target the technology, leading to risks such as personal data theft and biological threats.

A new study published in IEEE Access has revealed vulnerabilities in next-generation DNA sequencing (NGS) technology – a key tool in precision medicine, cancer research and infectious disease monitoring. Scientists warn that without improved security measures, hackers could target the technology, leading to risks such as personal data theft and biological threats.

NGS enables rapid and affordable DNA and RNA sequencing, driving advances in drug development, forensic science, and agriculture. However, the sequencing process involves complex steps such as sample preparation, sequencing, and data analysis. These steps rely on advanced tools, software, and connected systems, creating many opportunities for hackers to engage in malicious behavior such as falsifying genetic profiles or conducting unethical research.

Lead author of the study, Dr Nasreen Anjum from the School of Computer Science, University of Portsmouth (UK), highlighted the need for advanced security methods: "Our research is a wake-up call. Protecting genomic data is not just about encryption – it is also about anticipating attacks that have never existed before. We need a paradigm shift in how we secure the future of precision medicine."



The study highlights potential threats, including malware encoded in synthetic DNA data, AI-based manipulation of genomic data, and techniques to identify identities from genetic information. These risks go beyond the typical data breach, potentially harming individual privacy, scientific output, and even national

security. 'Genomic data is one of the most private forms of personal data we have. If compromised, the consequences would be far greater than a typical data breach.'

The study calls for urgent measures to improve cybersecurity in genomics. Suggested solutions include secure sequencing methods, encrypted data storage, and AI tools to detect anomalous activity. Dr. Anjum stressed the need for multidisciplinary collaboration between fields such as computer science, biotechnology, and security. She noted that experts in these fields often work in silos but must now work together for a common goal.

> Without concerted action, personal genomic data could be exploited for surveillance, discrimination, or even bioterrorism. Current protections are fragmented, leaving serious gaps in global biosecurity.

You finished reading the article "**Warning: Your DNA data can be hacked and misused**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com