Write-Up - Hacking Humans - Protecting our DNA from Cybercriminals

Arrington Goode

CYSE 495

3/19/2024

Bottom Line Up Front (BLUF)

After reading the article, “Hacking Humans: Protection Our DNA From Cybercriminals,” the amount of vulnerabilities that can be caused by DNA was brought to the forefront. The author Juliette Rizkallah explained in great detail how our DNA is being used and what can criminals do with it. The mixing of cybersecurity and biology has opened a lot of doors that can cause a variety of problems. For the everyday person, their data could be stolen and sold to anyone. An even more sinister application would be a criminal using your data to “prove” something about you that is not true. DNA is so useful because it directly identifies one individual person. However, if the DNA gets in the wrong hands it could prove to be catastrophic. There are ways to prevent this from happening such as only using online services you trust and being very intentional about how much of yourself you put online.

Introduction

The mixing of Cybersecurity and Biology into “Cyber Biosecurity” is a fast approaching world that many people are not ready to live in. Throughout the article titled “Hacking Humans: Protection Our DNA From Cybercriminals,” the author Juliette Rizkallah explains how the world is rapidly changing and how cybercriminals are ready to take advantage of this. One particular theme that was discussed in the article talks about this phenomenon and how far is too far. Once we start implementing DNA into everything, where do we draw the line? People will usually choose convenience over safety and this time it is no different. However, DNA is a very dangerous part of cybersecurity and it is still in the early stages. There are a multitude of ways that a cybercriminal could weaponize this data and exploit it.

DNA and Privacy

DNA, or deoxyribonucleic acid, is the most vital part of a human. In recent times, DNA has been used for different purposes. In the cybersecurity world, it can be used for a lot of different things including unlocking your phone or finding a suspect of a crime. In the process of using our DNA, we are giving up a piece of ourselves. At the end of the day, companies only really care about profits. However, it is not just companies that want to take advantage of the everyday person—a criminal will want to also. In an article by the Federal Trade Commission the author Elisa Jillson explains how vital DNA truly is. It can reveal information about a person’s medical history, their ancestry, and even things about their family. (Jillson)

When using your DNA, you are actively giving the other entity a vital piece of identifying information. This is a huge violation of your privacy and you should be able to give it

freely. However, there are companies who know the true value of DNA. They will send your data to other companies without permission and sell it in order to get more money. Data such as DNA is really valuable due to the fact that companies can directly see the type of people they are advertising to. On the opposite side of the spectrum, cybercriminals could use your DNA to steal personal information about an individual. Cybercriminals could also use DNA to falsely plant evidence and tamper with a crime scene. The amount of uses that DNA can have is extraordinary. In order to protect ourselves, we need to be more vigilant and do more research into the companies who have their hands in our data.

DNA and Cybercrime

When it comes to cyber crimes and how DNA can be used against you, the word "value" comes to mind. DNA is a resource that is practically invaluable. It is a direct link to someone and not many people can deny the validity of DNA. This makes it the golden ticket when it comes to criminals. Cyber crime is rising everyday. As time goes on, technology becomes more and more advanced. Due to this, many criminals are now becoming smarter. They understand that people will unknowingly use their own DNA without knowing the ramifications of doing that. In Jillson's article, they explain how companies will sell DNA based products in the hopes of turning a profit. If this is already happening within large companies then what is to stop one person from trying it? When you steal someone's data, you usually have near complete control over them and what they do online—without them even knowing it.

DNA can be used against you in a myriad of ways. Most people use DNA for security reasons. They use it as a way to unlock their devices and accounts. If someone were to get their

hands on this type of data, they would now have access to anything that the DNA could access. Bank accounts could be drained in seconds. Devices could be unlocked in seconds. All well guarded information is now in the hands of the criminal. The criminal could then hold that over the head of the victim or sell it to get their own profit. Even some companies are not above buying from criminals. It is a vicious cycle. Now that the door of cyber biosecurity is open, it exposes most of us to the true dangers of the internet. One danger of cyber biosecurity is the act of privacy and just how valuable it truly is. As stated earlier, privacy is a right that everyone should have. The internet has created an environment in which everyone is hypervisible at all times. That makes privacy all the more important. A person should be able to share only the information about themselves that they want to. A person should also be able to retract that information at any time and not have it in the hands of anyone. DNA is a phenomenal tool but it also can be a deadly one.

DNA and Cybercrime

The types of cybercrimes that are possible with DNA are frightening. An article by the Dark Reading Staff details a situation in which DNA was used in a cybercrime. It is just one example out of the many types of crimes that could occur. In this situation, the company "23andMe" was breached and lost a lot of their DNA data. Due to this, many people were put at risk. Their very personal information was exposed including their ancestry and even their geolocations. (Dark Reading, Staff) While nothing really dangerous occurred, that data has the potential to ruin everyone's life. If someone has your ancestry and your geolocation then they have the leverage over the consumer.

Conclusion

To conclude, DNA is a very dangerous resource. It has the potential to destroy countless lives. In today's time, the internet is rapidly changing and evolving. DNA is going to be used more and more. In order to properly protect ourselves from this change, we should really have better legislation to oversee this. The government has not yet dealt with the ramifications of DNA and cyber biosecurity. Aside from the governmental side, on the personal side we need to be more careful. Doing more research into the companies who have our DNA, only using our DNA on rare occasions, and learning from past mistakes will help keep us safe from any harm that may come our way.

References

Goodman, Marc, and Andrew Hessel. “DNA Hacking Is the Biggest Opportunity since Cyberattacks.” *Wired*, Conde Nast, 28 May 2013, www.wired.com/story/the-bio-crime-prophecy/.

Jillson, Elisa. “The DNA of Privacy and the Privacy of DNA.” *Federal Trade Commission*, 5 Jan. 2024, www.ftc.gov/business-guidance/blog/2024/01/dna-privacy-privacy-dna.

Rizkallah, Juliette. “Council Post: Hacking Humans: Protecting Our DNA from Cybercriminals.” *Forbes*, Forbes Magazine, 29 Nov. 2018, www.forbes.com/sites/forbestechcouncil/2018/11/29/hacking-humans-protecting-our-dna-from-cybercriminals/?sh=69a003165287.

Staff, Dark Reading. “23andMe Cyberbreach Exposes DNA Data, Potential Family Ties.” *Dark Reading*, Dark Reading, 8 Dec. 2023, www.darkreading.com/cyberattacks-data-breaches/23andme-cyberbreach-exposed-dna-data-family-ties.