OPEN ACCESS Freely available online

Journal of Research and Development

Review Article

Hacking Humans: The Art of Exploiting Psychology in the Digital Age

Cebo Daniel[1*], Jason R. Sipper[2]

[1]Department of Biotechnology and Medicine, Lifeboat Foundation, Nevada, USA; [2]Department of Biomedical Informatics, Ben-Gurion University, Negev, Israel

ABSTRACT

In our increasingly interconnected world, where technology permeates every aspect of our lives, the concept of hacking has expanded beyond traditional computer systems. Now, we find ourselves confronting the unsettling notion of hacking humans the manipulation and exploitation of individuals through psychological, social, and technological means. This emerging threat demands our attention as we navigate the complex landscape of human security in the digital age. As we continue to rely on technology in our daily lives, it is important to recognize the potential risks and vulnerabilities that come with it. Hacking humans poses a serious threat to our personal security and privacy, and it is essential that we remain vigilant and informed about the methods used by attackers. By taking steps to protect ourselves and staying up to date on the latest security measures, we can better safeguard our digital and physical well-being in this increasingly interconnected world.

Keywords: Cyberbiocrime, Hacking humans, Spam, Social engineering, Phishing, Digital footprints, Biohacking

INTRODUCTION

Biology and biotechnology have changed dramatically during the last ten years or so. Their reliance on digitization, automation, and their cyber-overlaps have created new vulnerabilities for unintended consequences and potentials for intended exploitation that are mostly underappreciated [1]. Hacking humans involves exploiting vulnerabilities in human psychology and behaviour to gain unauthorized access to sensitive information, manipulate opinions, or influence actions. It encompasses a wide range of tactics employed by cybercriminals and malicious actors, including social engineering, phishing, identity theft, and psychological manipulation [2]. The consequences of human hacking can be devastating, as they can lead to financial loss, reputational damage, and even physical harm. It is important for individuals and organizations to be aware of these tactics and take measures to protect themselves against them. This includes implementing strong security measures, educating employees and the public about these threats, and promoting digital literacy and critical thinking skills. For example, a common human hacking tactic is phishing, which involves sending fake emails or messages that appear to be from a trusted source in order to trick the recipient into revealing sensitive information such as login credentials or financial data. A recent example of this was the Google Docs phishing scam in 2017, where attackers sent emails that appeared to come from a known contact inviting users to collaborate on a document but instead led them to a fake login page where their credentials were stolen [3].

LITERATURE REVIEW

Methods of human hacking

Social engineering, one of the most prevalent forms of hacking, relies on psychological manipulation to deceive individuals into divulging confidential information or performing actions that compromise their security. Attackers may impersonate trusted individuals or organizations, exploit human emotions like fear or trust, or create a sense of urgency to persuade victims into providing access to sensitive data or systems. Social engineering is a common tactic used by cybercriminals to gain access to sensitive information or systems. By manipulating human emotions and exploiting trust, attackers can trick individuals into divulging confidential information or performing actions that compromise their security. Impersonating trusted individuals or organizations is a common technique, as it allows attackers to appear legitimate

Correspondence to: Cebo Daniel, Department of Biotechnology and Medicine, Lifeboat Foundation, Nevada, USA; E-mail: cebodaniel@humanacumen.info

Received: 06-Jun-2023, Manuscript No. JRD-23-24835; **Editor assigned:** 09-Jun-2023, PreQC No. JRD-23-24835 (PQ); **Reviewed:** 26-Jun-2023, QC No. JRD-23-24835; **Revised:** 03-Jul-2023, Manuscript No. JRD-23-24835 (R); **Published:** 10-Jul-2023, DOI: 10.35248/2311-3278.23.11.224

Citation: Daniel C, Sipper JR (2023) Hacking Humans: The Art of Exploiting Psychology in the Digital Age. J Res Dev. 10:224.

and trustworthy. Fear and urgency are also powerful motivators, as they can cause individuals to act impulsively without fully considering the consequences [4]. It's important for individuals and organizations to be aware of these tactics and take steps to protect themselves against social engineering attacks, such as implementing strong security protocols and educating employees on how to identify and avoid these types of scams.

Another method of human hacking is phishing, which involves sending fraudulent emails or messages that appear to come from a legitimate source, such as a bank or social media platform. These messages often contain a sense of urgency, prompting the recipient to click on a link or provide personal information. Once the victim falls for the scam, the attacker can gain access to sensitive data or install malware on the victim's device. To prevent falling for a phishing scam, it's important to verify the authenticity of the sender and to never click on suspicious links or provide personal information unless you are certain of the legitimacy of the request. These attacks often prey on human curiosity, fear of missing out, or the desire to help others, making individuals unwitting participants in their own victimization. For example, an attacker may pose as a CEO or other high-ranking official within a company and send an urgent email to employees requesting that they transfer funds to a certain account. The message may be convincing enough that some employees will follow through without verifying the request, resulting in a significant financial loss for the company [5]. Another example is when an attacker sends a fraudulent email claiming to be from a social media platform, alerting the recipient that their account has been compromised and prompting them to click on a link to reset their password. Once the victim clicks on the link and enters their login credentials, the attacker can gain access to their account and potentially steal personal information or use the account for further phishing attacks. It is important to always be cautious and sceptical of unsolicited messages, and to verify the authenticity of the sender and the request before taking any action [6,7].

Moreover, the rise of social media and the digital footprint individuals leave behind present opportunities for hackers to gather personal information and launch targeted attacks. Personal data shared online, such as birthdays, addresses, or workplace details, can be exploited to gain unauthorized access to accounts or commit identity theft, leading to financial loss and reputational damage. Furthermore, even seemingly harmless information like social media posts or online shopping habits can be used to create a profile of an individual's interests and behaviours, which can then be used for phishing scams or social engineering attacks [8-10]. For instance, a hacker can use information posted on social media, such as vacation plans or travel itineraries, to perform physical attacks like burglary or stalking. Additionally, when individuals fill out online surveys or submit personal information for promotions, they could unknowingly provide sensitive data that can be leveraged for phishing attacks or identity theft.

To mitigate these risks, individuals can take steps to minimize their digital footprint. This includes being mindful of the information shared on social media and other online platforms, using strong and unique passwords, enabling two-factor authentication, and regularly monitoring financial accounts for suspicious activity. Additionally, individuals can invest in reputable antivirus software and keep their devices up to date with the latest security patches. It is also important to educate oneself on common phishing scams and avoid clicking on suspicious links or downloading attachments from unknown sources. By taking these precautions, individuals can better protect themselves from the potential harm of a compromised digital footprint [11].

Furthermore, it is crucial to use strong and unique passwords for all online accounts and to enable two-factor authentication whenever possible. This adds an extra layer of security and makes it more difficult for hackers to gain access to sensitive information. Additionally, individuals should regularly back up important data to an external hard drive or cloud storage service in case of a cyber-attack or device failure [12,13]. It is also recommended to use a reputable antivirus software and keep it updated to detect and remove any malware or viruses. Lastly, individuals should be cautious when using public Wi-Fi networks and avoid accessing sensitive information such as bank accounts or personal emails while connected. By implementing these measures, individuals can significantly reduce their risk of falling victim to cybercrime and protect their digital identity.

Rising of biohacking

However, as technology continues to advance, a new form of cybercrime is emerging biohacking. Internet of Things (IoT) devices, wearable technologies, and smart home systems can be compromised, enabling unauthorized access to personal data, surveillance, or even control over essential systems like home security or medical devices. Bio-hacking involves the manipulation of biological systems using technology, and it has the potential to cause significant harm if not properly regulated. Hackers could potentially gain access to medical devices such as pacemakers or insulin pumps, causing serious harm or even death to the individual using them [14]. Additionally, genetic data could be stolen and used for nefarious purposes, such as insurance fraud or discrimination. As with traditional cybercrime, prevention is key. It is important for individuals to stay informed about the risks associated with bio-hacking and take steps to protect themselves. This may include using strong passwords and two-factor authentication on medical devices, avoiding sharing genetic data with untrusted sources, and advocating for stronger regulations on bio-hacking practices. By staying vigilant and proactive in our approach to cyber security, we can help ensure a safer digital future for all [15,16].

Furthermore, the growing field of bio-hacking raises concerns about the security and integrity of implanted medical devices or wearable implants. The potential for unauthorized access to personal data and surveillance is a growing concern, particularly when it comes to devices like wearable technologies and smart home systems. These devices can be easily compromised, leaving users vulnerable to cyber-attacks and privacy breaches. In addition, the rise of bio-hacking has raised questions about the security and integrity of implanted medical devices or wearable

implants. As more people begin to incorporate these technologies into their daily lives, it's important that manufacturers prioritize security measures to protect users from potential harm.

One of the biggest challenges in securing these devices is the sheer number of vulnerabilities that exist. Many Internet of Things (IoT) devices are built on outdated software and lack basic security features, leaving them open to attack. Additionally, the sheer variety of devices and manufacturers makes it difficult to implement universal security protocols. Despite these challenges, there are steps that can be taken to improve the security of these devices. Manufacturers can prioritize security in the design phase, while users can take steps to secure their devices through regular updates and strong passwords. Ultimately, it will take a collaborative effort between manufacturers, users, and policymakers to ensure that the benefits of these technologies are not outweighed by the risks they pose to personal security and privacy. As the field of bio-hacking continues to evolve, it is essential that we remain vigilant in addressing these security concerns to ensure the safety and well-being of all those who rely on these devices [17].

In 2017, the US Food and Drug Administration issued a recall for 465,000 pacemakers after discovering security vulnerabilities that could potentially allow hackers to tamper with the devices. The recall required patients to visit their doctors for a firmware update to improve security and prevent unauthorized access. Similarly, researchers have demonstrated how wearable health trackers can be hacked to falsify data, potentially leading to misdiagnosis or inadequate treatment if the data is relied upon by medical professionals. This highlights the growing concern about the security of medical devices and the need for improved measures to protect patient data [18,19]. While firmware updates are a step in the right direction, more comprehensive solutions are needed to address vulnerabilities in these devices. Additionally, there is a need for increased education and awareness among healthcare professionals and patients about the risks associated with wearable health trackers and other medical devices. As technology continues to advance, it is important that security measures keep pace to ensure patient safety and privacy. The healthcare industry must work together to develop robust security protocols that can withstand cyber-attacks and safeguard sensitive patient information. Only then can we truly harness the power of technology to improve healthcare outcomes while ensuring patient safety and privacy.

Safeguard against human hackers

One way to do this is by implementing multi-factor authentication for all healthcare staff accessing patient data. Additionally, regular security audits and risk assessments should be conducted to identify vulnerabilities and address them promptly. It is also important to educate patients on how to protect their personal health information, such as by using strong passwords and avoiding sharing sensitive information over unsecured networks. By taking these proactive measures, the healthcare industry can create a culture of security and privacy that benefits both patients and providers alike. Ultimately, this will lead to better healthcare outcomes and increased trust in the healthcare system. For example, a hospital could implement a system where all staff must use a physical token, such as a smart card or USB drive, to access patient records in addition to entering a password. This would greatly reduce the risk of someone accessing patient data without authorization. Additionally, regular security audits could reveal vulnerabilities such as outdated software or weak passwords that need to be addressed. By educating patients on the importance of security and privacy, they can become active partners in safeguarding their own health information.

To safeguard against the threats posed by hackers, individuals must adopt a proactive approach to personal security. Educating one-self about common hacking techniques, practicing strong password hygiene, and being vigilant when sharing personal information online are essential steps in protecting against cyber-attacks. It is crucial to question and verify requests for sensitive information, especially in unsolicited communications. Furthermore, individuals should regularly update their devices and software to ensure they have the latest security patches [20]. It is also recommended to use two-factor authentication whenever possible, as it adds an extra layer of protection. In addition, individuals should be cautious when using public Wi-Fi networks and avoid accessing sensitive information on them. Another important aspect of personal security is being aware of phishing scams and not clicking on suspicious links or downloading attachments from unknown sources. Lastly, it is essential to regularly back up important data to prevent loss in the event of a cyber-attack or device failure. By following these proactive measures, individuals can significantly reduce their risk of falling victim to cyber bio-crime.

Organizations also bear a responsibility to address the risks associated with hacking humans. Robust cyber security measures, regular employee training on social engineering techniques, and the implementation of strict data protection policies are crucial in fortifying defenses against human hacking attempts. Encouraging a culture of cyber security awareness and providing channels for reporting suspicious activities empowers individuals to contribute to a safer digital environment.

It is also important to conduct regular risk assessments and establish incident response plans to quickly address any potential breaches. Collaboration with industry experts and staying informed on emerging threats can also aid in staying ahead of potential attacks. Ultimately, a comprehensive approach to cyber security that prioritizes prevention, detection, and response is essential to safeguarding sensitive information and maintaining trust with customers and stakeholders. For example, a healthcare organization can implement robust cyber security measures by conducting regular risk assessments and providing employee training on social engineering techniques [21]. The organization can also establish incident response plans to quickly address any potential breaches and provide channels for reporting suspicious activities to promote a culture of cyber security awareness. By doing so, the organization can ensure the security and privacy of patient data and maintain trust with stakeholders.

Additionally, it is essential to invest in education and awareness programs that teach individuals how to protect themselves from

cyber threats. This includes teaching basic cyber security practices such as creating strong passwords, using two-factor authentication, and avoiding suspicious emails or links. Additionally, businesses and organizations must prioritize cyber security measures by implementing firewalls, antivirus software, and regular system updates. It is also important to conduct regular security audits to identify vulnerabilities and address them promptly. Finally, international cooperation is necessary to combat cybercrime on a global scale [22-26]. Governments should work together to share information and coordinate efforts to apprehend cybercriminals who operate across borders. By taking these steps, we can create a safer digital environment for individuals and businesses alike [27].

On top of that, legislation and regulations must keep pace with the rapidly evolving landscape of hacking. Authorities should work to create legal frameworks that deter cybercriminals and impose penalties for those who engage in malicious activities targeting individuals. Collaborative efforts between the public and private sectors are paramount to effectively combating this complex issue [28].

Moreover, it is crucial to establish clear laws and regulations that hold individuals and organizations accountable for their actions online. This includes penalties for cybercrime, as well as protection for individuals who report cyber threats or incidents. Governments should also invest in the development of advanced technologies and tools to detect and prevent cyber-attacks. This includes artificial intelligence and machine learning algorithms that can analyze large amounts of data to identify potential threats. In addition, there should be increased collaboration between law enforcement agencies and cyber security experts to improve response times and minimize the impact of cyber-attacks [29]. Overall, a multi-faceted approach is needed to effectively address the growing threat of cyber bio-crime. By implementing strong legal frameworks, fostering collaboration between the public and private sectors, investing in advanced technologies, and improving response times, we can better protect individuals and organizations from the devastating effects of cyber-attacks. It is important for governments and individuals alike to take this issue seriously and work together to create a safer and more secure online environment [30,31].

DISCUSSION

Hacking humans represents a significant and growing threat in the digital age. By exploiting our psychological vulnerabilities, attackers can bypass traditional security measures and gain unauthorized access to sensitive information. Understanding the tactics employed in hacking humans and fostering cyber security awareness are critical steps in mitigating this risk. Through a combination of individual vigilance, education, and organizational security measures, we can protect ourselves and our digital ecosystems from the perils of psychological manipulation. As we navigate the intricate challenges of the digital age, we must remain vigilant and informed about the risks associated with hacking humans. By embracing a proactive approach to personal security, fostering cyber security awareness, and advocating for robust safeguards, we can mitigate the threats posed by malicious actors. Together, we can create a safer digital environment that respects individual privacy and safeguards the integrity of our identities in this interconnected world. Furthermore, it is important to stay informed about the latest cyber security threats and best practices for protecting personal information. This can be achieved through attending workshops, reading articles, and following trusted cyber security experts on social media. By taking these steps, we can empower ourselves and others to stay safe online.

CONCLUSION

Moreover, it is essential to recognize that cyber biosecurity is not just an individual responsibility but also a collective one. Organizations must also take proactive measures to safeguard their networks and data from attacks. This includes implementing security protocols, conducting regular security audits, and providing cyber security training to employees. By creating a culture of cyber security within an organization, it becomes easier to detect and respond to threats quickly. In addition, it is crucial to stay up to date with the latest security technologies and trends to stay ahead of potential attackers. By working together, individuals and organizations can build a stronger defense against cyber threats and protect our digital world.

REFERENCES

1. Mueller S. Facing the 2020 pandemic: What does cyber-biosecurity want us to know to safeguard the future? Biosaf Heal. 2021;3(1):11-21.
2. Palmer XL, Potter L, Karahan S. An exploration on apts in biocybersecurity and cyberbiosecurity. Int Conf Cyb Warf Secur. 2022;17(1):532-535.
3. Cebo P. Cyberbiosecurity-It is time to take some intelligent decisions. SSRN Preprint. 2021.
4. Dixon TA. The bioinformational dilemma: where bio informational diplomacy meets cyber biosecurity. Austra J Int Aff. 2023;26:1-9.
5. Jordan SB, Fenn SL, Shannon BB. Transparency as threat at the intersection of artificial intelligence and cyberbiosecurity. Comp. 2020;53(10):59-68.
6. Mokhov AA, Svirin YA, Gureev VA, Sangadzhiev BV, Shestov SN. Diy biology and biohacking: Socio-legal aspect. J Adv Res Dynam Contrl Syst. 2020;12(S4):1620-1626.
7. Yetisen AK. Biohacking. Tren biotech. 2018;36(8):744-747.
8. Puchkov DV. Biohaking: For and against? Euras Leg J. 2021;(10):250-253.
9. Wright S. Biohacking queer and trans fertility: using social media to form communities of knowledge. J Med Humanit. 2023;26:1-9.
10. Mauger J. Religion and the technological future: an introduction to bio hacking, artificial intelligence and trans humanism. J Trothen Nova Religio. 2021;26(2):116-118.
11. Ordieres-Meré J, Gutierrez M, Villalba-Díez J. Toward the industry 5.0 paradigm: increasing value creation through the robust integration of humans and machines. Comp Indust. 2023;150:103947.
12. Schiller D. Neuroscience: Hacking the brain to overcome fear. Nat Hum Behav. 2016;1(1):0010.
13. Söderberg J, Delfanti A. Hacking hacked! The life cycles of digital innovation. Sci Tech Hum Val. 2015;40(5):793-798.
14. Ranjan D. Preventing Social Sites from Publishing Malicious Content. Int J Engine Comp Sci. 2016;5(10).

15. Akinyelu AA. Advances in spam detection for email spam, web spam, social network spam, and review spam: ML-based and nature-inspired-based techniques. J Comp Sec. 2021;29(5):473-529.
16. Liu X, Lu H, Nayak A. A Spam transformer models for SMS spam detection. IEEE Access. 2021;9:80253-80263.
17. Zieni R, Massari L, Calzarossa MC. Phishing or not phishing? A survey on the detection of phishing websites. IEEE Access. 2023;11:18499-18519.
18. Halevi T, Memon N, Nov O. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. phishing self-efficacy and vulnerability to spear-phishing attacks. SSRN Preprint. 2015.
19. Fissel ER, Lee JR. The cybercrime illusion: examining the impact of cybercrime misbeliefs on perceptions of cybercrime seriousness. J Criminol. 2023;26338076231174639.
20. Mohsin K. The internet and its opportunities for cybercrime-interpersonal cybercrime. SSRN Preprint. 2021.
21. Opriş C. Cybercrime evolution and current threats. Int J Inform Sec Cybercri (IJISC). 2022;11(1):41-48.
22. Tin D, Hata R, Granholm F, Ciottone RG, Staynings R, Ciottone GR. Cyberthreats: A primer for healthcare professionals. Ame J Emer Med. 2023; 68:179-185.
23. Guitton MJ, Fréchette J. Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy. Comp Hum Behav Rep. 2023;10:100282.
24. Desai S. Curbing modern cyberthreats. Comp Fraud Sec. 2023;2023(1).
25. Nayak P, Rakesh CH, Chandana AS, Chandana PT, Darshan S. Review paper on cyberbulling. Int J Adv Res Sci Commun Tech. 2023;3(2):495-503.
26. Lee S, Sungkyu L. A study on role types and related factors of cyberbullying in adolescents. Youth Welf Resh. 2022;24(2):119-146.
27. Stadnyk MM, Boychuk OI. The problems of youth aggression, bullyng and cyberbulling in modern Ukrainian society. Curr Prob Phil Socio. 2022;37:14-22.
28. Greenbaum D. Cyberbiosecurity-a new field to deal with emerging threats. 2023.
29. Nicholson DN, Alquaddoomi F, Rubinetti V, Greene CS. Changing word meanings in biomedical literature reveals pandemics and new technologies. Bio Data Min. 2023;16(1):16.
30. Freda PJ, Kranzler HR, Moore JH. Novel digital approaches to the assessment of problematic opioid use. Bio Data Min. 2022;15(1):1-6.
31. Sipper M, Moore JH. Conservation machine learning. Bio Data Min. 2020;13(1):1-4.