Cognitive Hacking and Social Engineering in Healthcare: Exploiting Human Behaviour

Raheemat Adefabi[1], Oludolamu Onimole[1], Abuh Ibrahim Sani[2], Valentine Okpalanozie[3], Ahmed Olabisi Olajide[2], Taiwo Oseni[4], Chimeziri Chima Iwuoha[5], Fatimah Eniafe[5], Xavier Palmer[6] and Lucas Potter[6]

[1]Teesside University, Middlesbrough, UK
[2]University of Bradford, UK
[3]TMF, Lagos, Nigeria
[4]University of Huddersfield, UK
[5]Young Cyber Talents, Nigeria
[6]BiosView, USA

raheematopeyemi@gmail.com
oludolamuonimole@gmail.com
saniabuh@gmail.com
valentineokpalanozie@gmail.com
olajideolabisia@gmail.com
taiwooseni0000@gmail.com
cchimaiwuoha@gmail.com
omobolanlezara@gmail.com

Abstract: Hacking medical facilities proves to be a profitable venture. An entire individual record, containing name, insurance number, address, and social services identifier, can fetch hundreds of dollars on the dark web. Researchers have demonstrated how data breaches affect health information technology investment and its impact on the broader economy. Due to the vast number of individuals accessing personal data and inadequate security measures, healthcare facilities are vulnerable targets for cyberattacks. However, that healthcare facilities are vulnerable targets for cyber-attacks is not completely accurate. When it comes to cyber security, this sector has significantly advanced compared to others. However, despite significant funds being allocated to antivirus software, enhanced network security, and improved cyber security measures, breaches continue to occur. Human error is only partially responsible for this. Cognitive hacking uses false information, psychological influence, and misinformation to shape opinions and decisions, which can result in harmful health effects and distrust in verification. Social engineering uses strategies like phishing, pretexting, and impersonation to manipulate people and obtain unauthorised entry to systems, medical records, or critical infrastructure. Cognitive hacking and social engineering take advantage of healthcare professionals' characteristics like trust, empathy, and obedience to authority in addition to demanding work conditions to circumvent standard cybersecurity protections. This study explores the tactics and outcomes of these people-focused attacks in healthcare, emphasising the mental influences that leave the industry vulnerable. It also investigates actual steps to take, such as educating employees, using multi-factor authentication, preparing for incidents, and implementing controlled access rules, which are crucial for strengthening healthcare facilities against these intricate risks. Healthcare organisations can enhance protection of patient data, uphold operational stability, and foster trusted patient-provider relationships by recognising and dealing with the human factor. It will also analyse how different implementation techniques influence incident reduction rates, behavioural changes, and security awareness. By adopting this approach, this body of work will provide practical solutions that enhance the resilience of healthcare infrastructure while safeguarding patients' personal information.

Keywords: Cognitive, Hacking, Social engineering, Healthcare, Exploiting, Human behaviour

1. Introduction

Cognitive hacking is an attack that targets human users' perceptions and behaviors rather than unauthorized access to computer systems (G. Cybenko et al., 2002). It uses misinformation to influence actions and bypass technical security measures (Cybenko et al., 2004). Historical examples, like the Trojan War, show that social engineering tactics remain effective today, allowing adversaries to manipulate individuals at low costs for significant outcomes (Bone, 2017). In cybersecurity, these tactics involve psychological manipulation to gain unauthorized access (Al-Thani, 2022-10-29). Current research focuses more on building secure systems against technical threats, often neglecting cognitive hacking risks, which are harder to mitigate (W. Chung et al., 2018).

1.1 Healthcare Sector Vulnerabilities

Healthcare data, including medical history and prescriptions, is crucial for patient care, but digitizing records raises significant privacy and cybersecurity concerns (Li et al., 2023). Cyberattacks can expose sensitive information, disrupt care, and threaten patient safety (Jalali et al., 2019). Patient records are particularly valuable to cybercriminals, who can sell this data for much more than credit card information (Williams et al., 2020). The healthcare sector is highly vulnerable; it accounted for 24% of all data breaches in 2018 (Jalali et al., 2019). By 2022, cyberattacks cost US healthcare providers $28.2 billion (Black Book Market Research, 2023), with breach costs escalating to $9.77 million per incident by 2024 (IBM, 2024). To protect healthcare data and services, the sector must prepare for cognitive attacks (He et al., 2021).

1.1.1 Human factors in cybersecurity

Organizations heavily depend on human interaction with systems to combat evolving security threats, highlighting the critical role of the human factor (Zimmermann et al., 2024). Social engineering attacks exploit emotions such as fear and curiosity, with tactics like name-dropping often used to elicit sensitive information (Wang et al., 2021b). In healthcare, many data breaches stem from human error rather than technical vulnerabilities (Cartwright, 2023). Hackers frequently target users who engage in poor cyber hygiene, whether through the accidental disclosure of personal information or failure to adhere to guidelines (Kioskli et al., 2023). While some cybersecurity incidents result from intentional insider threats, many arise from unintentional actions that create vulnerabilities (Lynne et al., 2020). The fallibility of human users is a primary target for cyberattacks (Wiederhold, 2014). Variations in individual cyber hygiene can lead to unfavorable outcomes, often influenced by stress, workload, and situational awareness (Kioskli et al., 2023). Cybersecurity, as a complex socio-technical system, must increasingly incorporate human factors to tackle emerging challenges (Nobles, 2022). Furthermore, healthcare IT investment is needed to address both human and technical issues; in the UK, only 1–2% of the annual budget is dedicated to IT, compared to 4–10% in other sectors (Saira et al., 2019).

2. Literature Review

2.1 Social Engineering in Healthcare

Our research investigates cognitive hacking in healthcare, primarily focusing on social engineering cyber-attacks. Syafitri et al. (2022) highlighted that these attacks exploit the vulnerabilities of medical staff, emphasizing human weaknesses over technical flaws. Greavu-Şerban & Constantin (2022) explained that social engineering involves psychological manipulation to alter individuals' perceptions and beliefs. The sensitive data in healthcare makes it a prime target for hackers (Priestman et al., 2019). Trust in technology poses a significant challenge, leading to physical and social manipulation by hackers (Abbass et al., 2018). Social engineering tactics are especially effective in healthcare, as they exploit the vulnerabilities of both patients and staff (Khera, 2017). Salama & Al-Turjman (2023) noted that social engineers use psychological tactics like urgency and fear to extract sensitive information from healthcare staff. Partel (2022) argued that social engineering is a strategy that capitalizes on the trust inherent in human interactions, which hackers exploit for their gain (Salaheddine & Kaabouch, 2019).

2.1.1 Common attack techniques

The healthcare sector faces significant risks from social engineering attacks, as highlighted by Partel (2022). These attacks typically utilize physical, social, and reverse social engineering tactics, with the social approach being the most common due to its reliance on building trust (Salaheddine & Kaabouch, 2019). Common methods include phishing, vishing, shoulder surfing, and impersonation, with phishing being particularly prevalent for stealing sensitive medical records (Nadeem et al., 2023). Social engineering exploits vulnerabilities, leading employees to accidentally disclose sensitive information (Wang et al., 2021). The rise of IoT devices and the impact of the COVID-19 pandemic have further intensified this threat (Cartwright, 2023). Ultimately, social engineering poses a significant danger not only to individual patients but also to the overall healthcare system (Partel, 2022).

2.1.2 Trust dynamics in healthcare

The importance of healthcare trust cannot be understated. Trust is one prerequisite in the relationship between a patient and a healthcare professional and collaborating healthcare professionals. The fact remains that when there is no prior relationship or familiarity between the health provider and the patient, incipient trust in the healthcare system is what bridges the gap and removes the doubt between the two parties. In healthcare, trust is bidirectional in the sense that the patient must trust the health provider, and the healthcare must trust the

patient. The reason is that the patient cannot empirically trust the health provider's qualifications and precedents, but trust will encourage the patient to narrate his or her health conditions in a way the health provider can deduce the illness and proffer solutions. On the part of the healthcare provider, he or she should trust the patient, knowing that what he or she has said is exactly the condition, as this will make the healthcare provider offer a long-term solution. In essence, trust aids the communication between the patients and the healthcare provider, as both need to trust each other for proper communication (Rasiah et al, 2020). Not only does it facilitate communication but trust also influences the outcome of the treatment being provided by healthcare (Moudatsou et al, 2020).

2.1.3 Authority and compliance patterns

Healthcare, unlike other organizations, operates under authority, which is born out of hierarchy. For any organization to function well and effectively, there must be a recognized authority operating out of an established hierarchy. This is because, at the chain of command, the leadership has the responsibility to support and guard the lowest level. In the healthcare sector, the idea of hierarchy is divided into two: Flat and traditional hierarchy, with the flat hierarchy gaining more popularity in recent times (Fernandopulle, 2021). A flat hierarchy eliminates the idea of middle management between the leadership and the lowest level of the command chain, unlike the traditional hierarchy, which does not. The massive adaptation of the flat hierarchy is a result of the leadership, which is the executive, having full access to the employees without any obstruction from the middle management (Fernandopulle, 2021). This in turn helps to eliminate time wasting and fosters flexibility during any decision-making on a patient's health. This means that the employees are under the authority of the executives, thereby complying with any directives from the executive.

3. Methodology

3.1 Attack Vector Analysis

According to Koyun and Al-janabi 2017, human error is one of the main flaws in every organisation's cybersecurity plan. Social engineering attacks exploit this weakness by tricking individuals into compromising security and divulging private information. In the book "The Art of Deception", Kevin Mitnick described the four phases of the social engineering attack cycle. This includes a perpetrator gathering background information, gaining the victim's trust, and providing incentives for actions breaking security practices, such as revealing sensitive information or granting access to critical resources. Hence every social engineering attack includes one or more of these steps. This article will explore the different types of social engineering attacks.

Various types of social engineering attacks are:

Phishing: Phishing is the most common social engineering attack. According to the National Cyber Security Centre, the number of phishing reports as of October 2024 is over 36 million. Gupta et al. described phishing as a network attack in which an attacker produces a fake of an existing webpage to trick an internet user into disclosing personal information (Gupta, Singhal and Kapoor, 2016). Thus, with phishing, an attacker draws the victim in by impersonating a reputable source and making an intriguing request, just like a fisherman uses bait to capture a fish. Phishing can be in various forms and can be used to manipulate individuals or organisations differently. This includes Email phishing, Spear Phishing, Smishing, Vishing, Whaling, Angler Phishing etc.

Tailgating: This type of attack is also called piggybacking. The attacker follows an authorised person to gain access into areas they are unauthorised to visit. In most cases, this is to gain access to top-secret information or valuable assets (Syafitri et.al 2022). Tailgating can include an attacker impersonating a technician and following an employee into a security perimeter building. Another example is when an employee leaves the computer without locking in while logged into a private network. With the computer not locked, another employee with no authorised access can access the private network and its information.

Quid Pro Quo: This type of social engineering attack uses the principle of reciprocity to trick people into divulging information or carrying out activities against established security procedures. The attack entails providing a perceived benefit in return for sensitive information or access. This could be a reward or royalty promised by the attacker to the target (Salaheddine and Kaabouch, 2019).

Watering Hole Attack: According to the National Cyber Security Center, the watering hole attack is often found on websites visited by individuals inside a certain business or sector, such as defence, government, or healthcare. The website is then hacked to allow the deployment of malware. These attacks mostly target government

personnel since hacking into the government sector is extremely tough and risky. Watering hole attacks are infrequent and extremely effective due to their difficulty in detection (Lohani, 2019).

3.2 Psychological Triggers

Human cognition may be manipulated using strategies that target psychological weaknesses, biases, and how individuals process information. These strategies are intended to trick people into disclosing sensitive information, making poor judgements, or acting in ways that favour the enemies (Montanez, Golob and Xu, 2020). Human vulnerabilities can be exploited from thinking, imagining, knowing, hoping, dreaming, judging, remembering and solving problems, making healthcare a focus for these attacks (Wang, Zhu and Sun, 2021). In healthcare, trust can be compromised by cognitive hacking. An example of this is when people provide false information regarding vaccinations or treatments that might harm public health decisions. These strategies use psychological triggers, instinctive reflexes, or mental shortcuts to affect how people respond to specific situations (Budimir et al., 2021).

- Fear and Urgency: Healthcare personnel are mostly vulnerable to urgent requests due to their high-stress, fast-paced work environment. A hacker may utilise fear-based messaging, such as false ransomware assaults or bogus notifications about system breakdowns, to trick employees into taking urgent, unconfirmed action (Owen, 2024). Fear works together with urgency to compel immediate action. By creating a sense of imminent danger, attackers reduce the likelihood that the target will scrutinize the situation. Attackers instil a sense of urgency or fear to activate hasty, careless decisions. Urgency might cloud judgment, leading to hasty judgements, including releasing sensitive information. It activates the 'fight or flight' reaction, requiring people to make quick decisions to reduce perceived risks.
- Sense of Authority: Compliance is almost certain when someone is seen as someone in place of authority. Social engineers can take advantage of this by posing as senior medical consultants to lure healthcare assistants to give out patient information. Healthcare personnel have been trained to prioritise patient care and believe in authoritative sources. Cognitive hacking exploits this by mimicking trustworthy people, such as top administrators, regulatory authorities, or patients, to harvest sensitive information or gain unauthorised system access. For example, Jacintha Saldanha, a nurse at King Edward VII Hospital in London, committed suicide in December 2012 after answering a prank call from Australian radio hosts Mel Greig and Michael Christian, who pretended to be Queen Elizabeth and Prince Charles and enquired about the health of Catherine, Duchess of Cambridge, a hospital patient (Davies, 2014).
- Scarcity and Overload: According to cyberpsychology and cognitive psychology studies, tight deadlines and high workloads bring about speedy decision-making, which gives rise to an increase in the chance of mistakes such as misconfigurations, missed alarms, and delayed threat responses (Burrell, 2024). Scarcity is based on the idea that when resources, time, or opportunity are limited, people feel forced to act fast or prioritise certain actions, frequently bypassing logical decision-making. Social engineers exploit this by instilling a feeling of urgency in phishing emails or false phone calls, pushing hasty judgements without confirming authenticity. Overload occurs when an individual is bombarded with too much information, obligations, or stimuli, affecting their capacity to absorb material efficiently or make sensible judgements. Healthcare practitioners are frequently needed to perform numerous activities, such as caring for patients, updating records, and reacting to important contacts. During the COVID-19 epidemic, scarcity-driven attacks included lengthy emails announcing restricted vaccination appointments, enticing victims to disclose personal information or download malicious programs.
- Social Proof and Peer Influence: Social proof is the tendency to emulate others' behaviours or decisions, thinking they reflect proper behaviour. Social engineers may mimic trusted authorities or coworkers, such as a senior doctor or administrator, engage in fraudulent compliance practices, or abuse group norms (McAlaney, Thackray and Taylor, 2016). Peer influence is the subtle or overt pressure to conform to coworkers' or other healthcare professionals' acts, attitudes, or expectations. Healthcare workers may cooperate with phoney requests out of fear of being viewed as a hindrance to progress or unprofessional. Attackers might hack into collaborative systems to persuade healthcare personnel to make fake announcements or instructions that appear to come from colleagues.
- Reciprocity: Reciprocity stems from a sense of responsibility to reciprocate favours. Hackers may offer free services or products in exchange for access to data. In the healthcare industry, providing anything ostensibly advantageous, such as free tools, resources, or critical patient data, can instill a sense of

duty (Happa) (Happ,Melzer and Steffgen,2016). Also, reciprocity can include a reciprocal sharing of information and expertise. For example, hackers may transmit malware disguised as free medical software or updated treatment recommendations, taking advantage of experts' kindness and feeling of duty.

3.3 Impact Assessment of Psychological Triggers

The Impact Assessment of Psychological Triggers (Figure 1) includes how these psychological triggers can be maximised positively, thereby minimising the negative impacts of these triggers that give rise to cognitive hacking and social engineering in the healthcare sector. When used with psychological triggers of cognitive hacking, impact assessment serves a dual purpose: reducing the efficacy of such triggers while also addressing weaknesses inside the organisation.

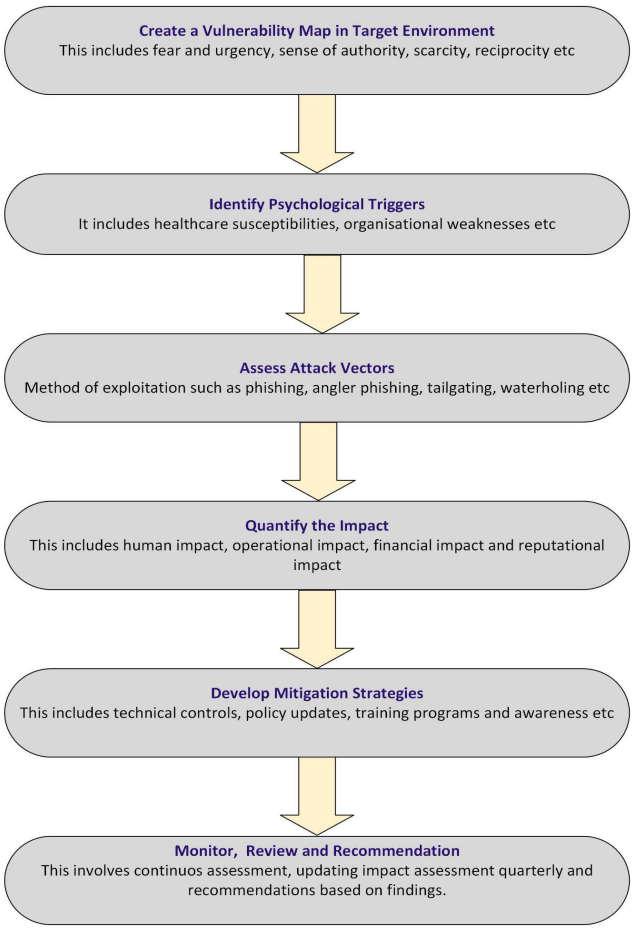

Figure 1: Flowchart of Impact Assessment

3.4 Defense Framework Development

- Employee education strategies: Cybersecurity education techniques include various instructional methodologies to effectively engage personnel. Options may include interactive workshops, online training courses, simulated phishing activities, and gamified learning platforms. Healthcare organisations should establish frequent training programs to educate personnel about cybersecurity best practices (Clarke and Martin, 2023). In research by Temitayo et al., 2024, the psychological and behavioural components of engagement, determining how motivating variables and personalised learning experiences lead to increased cybersecurity awareness, were investigated (Temitayo Oluwaseun, Abrahams et al., 2024). To ensure the effectiveness of this training, management should ensure the educational training program is tailored to each individual. Even though this might be expensive, it is the best approach to mitigate cognitive hacking and social engineering in the healthcare sector. Regular training sessions and simulated phishing drills help staff detect and avoid possible cyber-attacks.

- Authentication mechanisms: Endpoints, such as laptops, cellphones, and IoT devices, are the prime targets for cyber-attacks, particularly as remote work becomes more common in the healthcare industry (Pureti, 2023). A multifaceted approach is required to secure various endpoints. This plan should incorporate next-generation antivirus software, frequent software upgrades, multi-factor authentication, and endpoint detection and response (EDR) solutions (Omotunde & Ahmed, 2023). A multi-factor strategy is necessary for secure authentication.
- Access control policies: These policies will allow authorised network users in the healthcare sector to get access while excluding users who do not have the necessary credentials or rights (Golightly et al.,2023). Access control solutions enable organisations to safeguard sensitive data without impacting the user experience of workers or clients (Burrell, 2023). This includes role-based access control and least privilege access control. A policy of least privilege is a key notion in cybersecurity that restricts users' access permissions to those required for their job tasks. This principle seeks to reduce the possibility of unintentional or purposeful abuse of sensitive information and systems (Siwar 2024).

4. Discussion and Conclusion

As cyber threats evolve, the risks associated with cognitive hacking in healthcare have intensified. Attackers often exploit human error, leveraging psychological triggers such as fear, urgency, or authority to manipulate healthcare professionals into breaching security measures. This highlights the critical need for robust defenses for technological and human vulnerabilities. Human factors such as cognitive overload, stress, and the fast-paced nature of healthcare environments exacerbate the risk of falling victim to social engineering tactics. Hackers frequently exploit these conditions through phishing schemes, impersonation, and other psychological tactics, often compromising sensitive information and eroding trust in healthcare systems (Salahdine & Kaabouch, 2019; Patel, 2020). Moreover, trust, a cornerstone of patient-provider relationships, becomes a double-edged sword when attackers exploit it to access sensitive information. This manipulation not only leads to identity theft or data breaches but also damages public confidence in the integrity of healthcare systems (Moudatsou et al., 2020; Gomide et al., 2021) Behavioral studies consistently reveal the role of cognitive biases such as authority bias, social proof, and decision fatigue in increasing susceptibility to cyberattacks (Kioskli et al., 2023). Healthcare professionals, burdened by demanding workloads, often lack the resources to thoroughly evaluate potential threats, making them prime targets for social engineering. Addressing these risks requires cybersecurity frameworks integrating human behavioral insights to mitigate cognitive vulnerabilities.

4.1 Conclusion

Cognitive hacking and social engineering attacks represent a growing and pervasive threat to the healthcare industry. The interplay between technical vulnerabilities and human factors, such as stress and cognitive overload, amplify the risk of data breaches and system compromises. However, understanding the psychological aspects of these attacks enables healthcare organizations to design tailored defenses. Adopting a socio-technical approach combining behavioral insights with advanced security protocols, healthcare institutions can enhance resilience against cognitive hacking. This not only reduces the effectiveness of social engineering tactics but also fosters a culture of cybersecurity awareness among healthcare professionals. Ultimately, mitigating both technical and human vulnerabilities is essential to safeguarding patient data and ensuring trust in modern healthcare systems.

References

Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O. (no date) 'CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY'. Available at: https://doi.org/10.51594/csitrj.v5i.708.

Al-Thani, N. A. (2022-10-29). Adolescents' and social engineering: The role of psychometrics factors in determining vulnerability and designing interventions. Paper presented at the *2022 9th International Conference on Behavioural and Social Computing (BESC),* 10.1109/besc57393.2022.9995705

Birkhäuer, J., Gaab, J., Kossowsky, J., Hasler, S., Krummenacher, P., Werner, C., and Gerger, H. (2017) 'Trust in the healthcare professional and health outcome: A meta-analysis,' PLOS ONE. doi: 10.1371/journal.pone.0170988.

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *Journal of Medical Systems, 44*(5)10.1007/s10916-019-1507-y

Black Book Market Research. (2023). *2024 State of the Healthcare Cybersecurity Industry; Q4 2023 User Survey Results.* .Black Book Market Research LLC. https://blackbookmarketresearch.com/images/2024-State-of-the-Cybersecurity-Industry-01-12-23.pdf

Bone, J. (2017). *Cognitive Hack: The New Battleground in Cybersecurity… the Human Mind 10.1201*/9781315368412

Budimir, S., Fontaine, J.R.J., Huijts, N.M.A., Haans, A., Loukas, G. and Roesch, E.B. (2021) 'Emotional Reactions to Cybersecurity Breach Situations: Scenario-Based Survey Study'. JMIR Publications Inc. (Journal of Medical Internet Research, 23). Available at: https://doi.org/10.2196/24879.

Burrell, D.N. (2023) 'Cybersecurity in Healthcare Through the 7-S Model Strategy', 28(1), p. 26. Available at: https://doi.org/10.2478/bsaft-2023-0003.

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing, 37*(5), 1123. 10.1007/s10877-023-01013-5.

Clarke, M. and Martin, K. (2023) 'Managing cybersecurity risk in healthcare settings'. SAGE Publications (Healthcare Management Forum, 37). Available at: https://doi.org/10.1177/08404704231195804.

Cybenko, G., Giani, A., & Thompson, P. (2004). Cognitive Hacking. *Advances in Computers, 60*, 35–73. 10.1016/S0065-2458(03)60002-1

David, U.G. and Bode-Asa, A., 2023. An Overview Of Social Engineering: The Role of Cognitive Biases Towards Social Engineering-Based Cyber-Attacks, Impacts and Countermeasures. network, 23, p.24.

Davies, C. (2014) 'Jacintha Saldanha "took blame" for Duchess of Cambridge prank call', 11 September. Available at:https://www.theguardian.com/world/2014/sep/11/jacintha-saldanha-took-blame-prank-call-duchess-cambridge-australian-djs-inquest (Accessed: 19 January 2025).

Fernandopulle, N. (n.d.) 'To what extent does hierarchical leadership affect health care outcomes?' Medical Journal of The Islamic Republic of Iran (MJIRI), 2020, pp. 1–3.DOI: 10.1145/302979.302991

G. Cybenko, A. Giani, & P. Thompson. (2002). Cognitive hacking: a battle for the mind. *Computer, 35*(8), 50–56. 10.1109/MC.2002.1023788

Golightly, L., Modesti, P., Garcia, R. and Chang, V. (2023) 'Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN', 1. Available at: https://doi.org/10.1016/j.csa.2023.100015.

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science, 181*, 59. 10.1016/j.procs.2021.01.103

Greavu-Şerban, V. and Constantin, F., 2022. Aspects of Social Engineering and Its Modalities to Counter Charge and Prevent It. Informatica Economica, 26(3).

Gupta, S., Singhal, A. and Kapoor, A. (2016) A Literature Survey on Social Engineering Attacks: Phishing Attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 29-30 April 2016, 537-540.https://doi.org/10.1109/CCAA.2016.7813778

H. Abie. (2019). Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems. Paper presented at the *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT),* 1–6. 10.1109/ISMICT.2019.8743670.

Happ, C., Melzer, A. and Steffgen, G. (2016) 'Trick with treat – Reciprocity increases the willingness to communicate personal data', 61, p. 372. Available at: https://doi.org/10.1016/j.chb.2016.03.026

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). *Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review*. JMIR Publications Inc. 10.2196/21747

Hijji, M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access, 9*, 7152. 10.1109/access.2020.3048839

IBM. (2024). Cost of a Data Breach Report 2024. . United States: IBM. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). *Health Care and Cybersecurity: Bibliometric Analysis of Literature*. JMIR Publications Inc. 10.2196/12644

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. 10.1016/j.cose.2021.102267

Khera, M., 2017. Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. Journal of diabetes science and technology, 11(2), pp.207-212.

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Applied Sciences, 13*(6)10.3390/app13063410

Koyun, A. and Al Janabi, E., 2017. Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST), 4*(6), pp.7533-7538.

Li, Y., Yang, J., Zhang, Z., Wen, J., & Kumar, P. (2023). Healthcare Data Quality Assessment for Cybersecurity Intelligence. *IEEE Transactions on Industrial Informatics, 19*(1), 841. 10.1109/tii.2022.3190405

Lohani, Shivam, Social Engineering: Hacking into Humans (February 5, 2019). International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 2019, Available at SSRN: https://ssrn.com/abstract=3329391

Longtchi, T.T., Rodriguez, R.M., Al-Shawaf, L., Atyabi, A. and Xu, S., 2024. Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey. Proceedings of the IEEE.

Lynne, C., Dawn, B., Elizabeth, S., Sabina, M., Pasquale, M., Aimilia, M., & Kalliopi, A. (2020). *HCI for Cybersecurity, Privacy and Trust*. Springer. https://doi.org/10.1007/978-3-030-50309-3_8

Lundie, M., Lindke, K., Amos-Binks, A., Aiken, M.P. and Janosek, D., 2024, January. The Enterprise Strikes Back: Conceptualizing the HackBot-Reversing Social Engineering in the Cyber Defense Context. In HICSS (pp. 984-993).

Mcalaney, J., Thackray, H. and Taylor, J. (2016) 'The social psychology of cybersecurity'.

Montañez, R., Golob, E. and Xu, S., 2020. Human cognition through the lens of social engineering cyber attacks. Frontiers in psychology, 11, p.1755.

Moudatsou, M., Stavropoulou, A., Philalithis, A., and Koukouli, S. (2020) 'The role of empathy in health and social care professionals,' Healthcare, 8(1), pp. 1–3. doi: 10.3390/healthcare8010026.

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health Authors. *International Journal for Quality in Health Care, 3*(1)10.1093/intqhc/mzaa117

Nadeem, M., Zahra, S.W., Abbasi, M.N., Arshad, A., Riaz, S. and Ahmed, W., 2023. Phishing attack, its detections and prevention techniques. International Journal of Wireless Security and Networks, 1(2), pp.13-25p.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors, 21*(15), 5119–5139. https://doi.org/10.3390/s21155119

Nifakos, S., Chandramouli, K. and Stathakarou, N., 2024. Social Engineering: The Human Behavior Impact in Cyber Security Within Critical Information Infrastructures. In Security and Privacy in Smart Environments (pp. 173-184). Cham: Springer Nature Switzerland.

Okafor, C. M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, L., Onunka, O., & Omotosho, A. (2023). Mitigating Cybersecurity Risks in the U.S. Healthcare Sector. *International Journal of Research and Scientific Innovation (IJRSI), X*(IX), 177–191. https://doi.org/10.51244/IJRSI.2023.10918

Omotunde, H. and Ahmed, M. (2023) 'A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond'. Available at: https://doi.org/10.58496/MJCS/2023/016.

Patel, N., 2020. SOCIAL ENGINEERING AS AN EVOLUTIONARY THREAT TO INFORMATION SECURITY IN HEALTHCARE ORGANIZATIONS. Jurnal Administrasi Kesehatan Indonesia, 8(1), 56. https://doi.org/10.20473/jaki.v8i1.2020.56-64

Priestman, W., Anstis, T., Sebire, I.G., Sridharan, S. and Sebire, N.J., 2019. Phishing in healthcare organisations: Threats, mitigation and approaches. BMJ health & care informatics, 26(1).

Pureti, N. (2023) 'Strengthening Authentication: Best Practices for Secure Logins'.

Qureshi, S. (2024) 'Establishing a Policy of Least Privilege: The Impact of Segregation of Duties on Cyber Defense'. Available at: https://doi.org/10.13140/RG.2.2.34654.04163.

Rasiah, S., Jaafar, S., Yusof, S., Ponnudurai, G., Chung, K.P.Y., and Amirthalingam, S.D. (2020) 'A study of the nature and level of trust between patients and healthcare

Saira, G., Emilia, G., Nick, J., & Ara, D. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health, 1*(1), e10–e12. 10.1016/S2589-7500(19)30005-6

Salaheddine, F. and Kaabouch, N., 2019 'Social Engineering Attacks: A Survey', Future Internet, 11(89), pp.–17. doi: 10.3390/fi11040089.

Salama, R. and Al-Turjman, F., 2023. Cyber-security countermeasures and vulnerabilities to prevent social- engineering attacks. In Artificial Intelligence of Health-Enabled Spaces (pp. 133-144). CRC Press.

Swargiary, K., 2024. Techniques for Manipulation and Mind Control. ERA, US.

Syafitri, W., Shukur, Z., Asma Mokhtar, U., Sulaiman, R. and Ibrahim, M.A., 2022. Social engineering attacks prevention: A systematic literature review. IEEE access, 10, pp.39325-39343.

W. Chung, J. Liu, X. Tang, & V. S. K. Lai. (2018). Extracting Textual Features of Financial Social Media to Detect Cognitive Hacking. Paper presented at the *2018 IEEE International Conference on Intelligence and Security Informatics (ISI),* 244–246. 10.1109/ISI.2018.8587364

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access, 8*, 85094. 10.1109/access.2020.2992807

Wang, Z., Zhu, H., & Sun, L., (2021a). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access, 9, 11895–11910. https://doi.org/10.1109/access.2021.3051633

Wang, Z., Zhu, H., & Sun, L. (2021b). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access, 9*, 11895. 10.1109/access.2021.3051633

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research, 22*(9)10.2196/23692

Zimmermann, V., Schöni, L., Schaltegger, T., Ambuehl, B., Knieps, M., & Ebert, N. (2024, -10-25). Human-Centered Cybersecurity Revisited: From Enemies to Partners. *Communications of the ACM, 67*, 72. 10.1145/3665665