JAKI
JURNAL ADMINISTRASI KESEHATAN INDONESIA
INDONESIAN JOURNAL of HEALTH ADMINISTRATION

Jurnal Administrasi Kesehatan Indonesia Volume 8 No 1 June 2020
Published by Universitas Airlangga
Doi:

COMMENTARY ARTICLE

SOCIAL ENGINEERING AS AN EVOLUTIONARY THREAT TO INFORMATION SECURITY IN HEALTHCARE ORGANIZATIONS

Social Engineering sebagai Ancaman Evolusioner terhadap Keamanan Informasi dalam Organisasi Pelayanan Kesehatan

***Naiya Patel[1]**
[1]School of Public Health and Information Science, University of Louisville, United States
*Correspondence: naiya.patel2014@gmail.com

ABSTRACT

Information security in healthcare settings is overlooked even though it is the most vulnerable for social engineering attacks. The theft of hospital information data is critical to be monitored as they contain patients' confidential health information. If leaked, the data can impact patients' social as well as professional life. The hospital data system includes administrative data, as well as employees' personal information hacked, which can cause identity theft. The current paper discusses types and sources of social engineering attacks in healthcare organizations. Social engineering attacks occur more frequently than other malware attacks, and hence it is crucial to understand what social engineering is and its vulnerabilities to understand the prevention measures. The paper describes types of threats, potential vulnerabilities, and possible solutions to prevent social engineering attacks in healthcare organizations.

Keywords: social engineering, hospitals, healthcare organizations, information security.

ABSTRAK

Keamanan informasi pada bidang pelayan kesehatan terlalu dikesampingkan meskipun aspek ini merupakan aspek paling rentan terkena rekayasa sosial. Pencurian data informasi rumah sakit penting untuk diawasi karena informasi semacam itu mengandung informasi rahasia kesehatan pasien, yang bisa memengaruhi kondisi sosial dan kehidupan profesional pasien jika rahasia tersebut terbuka. Sistem data rumah sakit seperti data asministrasi dan informasi pribadi pegawai, yang dicuri dapat menyebabkan pencurian identitas. Artikel ilmiah ini membahas tentang tipe-tipe dan sumber pencurian data dalam organisasi kesehatan. Pencurian data lebih sering terjadi dari pada serangan virus lainnya, sehingga penting untuk memahami pengertian rekayasa sosial dan kerentanannya sebagai usaha memahami cara pencegahannya. Artikel ini membahas juga jenis ancaman, kerentanan yang potensial, dan solusi yang mungkin diambil untuk mencegah serangan rekayasa sosial dalam organisasi kesehatan.

Kata kunci: *rekayasa sosial, rumah sakit, organisasi kesehatan, keamanan informasi.*

Received: 9 November 2019 ***Accepted: 20 January 2020*** ***Published: filled by admin***

INTRODUCTION

Social engineering is an extraordinarily tricky manipulation performed by hackers to gain unauthorized access to data or systems, which they are not authorized to. It is a well-planned strategy to exploit the "trust" factor amongst human beings. People would easily trust a stranger if asked for help and would be willing to help them. Hackers, on the other side, would benefit from such kindness factor and abuse it (Salahdine and Kaabouch, 2019).

In today's fast-paced world, every employee in industry, business or professional organizations is turning towards being flexible and is more susceptible to use personal phones or devices for accessing company or enterprise information (Krombholz, Hobel, Huber, and Weippl, 2015). Opening up the options for communication channels like web 2.0, which includes Facebook and Twitter as well as another internet resource, we are increasing our susceptibility to data theft and security breach in healthcare settings. Allowing individual hospital/healthcare information establishment to be available on the public domain might pose severe threats to the enterprise from hackers attacks. Several organizational theories, including Structural Contingency Theory and Transaction Cost Theory, describe how technological innovations cause a change in healthcare organizational structures (Mick and Shay, 2014). They include installing a new software program in the hospital database for improved efficiency like the EPIC system or buying a new technology in general.

The current paper explores one such aspect of healthcare organizations, the hospital information system security. Lots of studies talked about information security and its essentiality for different corporate business settings or government institutions, but much less of a focus is on hospital information system security which includes, patients' electronic medical records, hospital administration information, as well as general technology information relevant to employee access, and employee payroll. Social engineering is one of the aspects which needs attention in the healthcare sectors, such as pharmaceutical industry which conduct clinical trials, hospitals, health insurance companies, private and government-funded dental clinics and general health clinics that have sensitive patients' health information. It is vital to understand types of social engineering attacks, as well as its possible approaches in less researched fields of healthcare where patients' private information is at most prone to identity theft and tampering (Conteh and Schmick, 2016). Globally this area of information security has advanced from installing antivirus to proactive employee training and awareness regarding susceptibility and forms of social engineering attacks. Governing bodies of respective countries have also set specific standards and penalties if patients' information data are not protected and breached. However, with continuously evolving resources and types of social engineering attacks, it is essential to understand different types and sources of social engineering attacks. The objective of the current paper is to address these questions. It further discusses different healthcare settings which are potentially susceptible to the theft of patients' health data and provide possible solutions.

APPROACHES AND TYPES

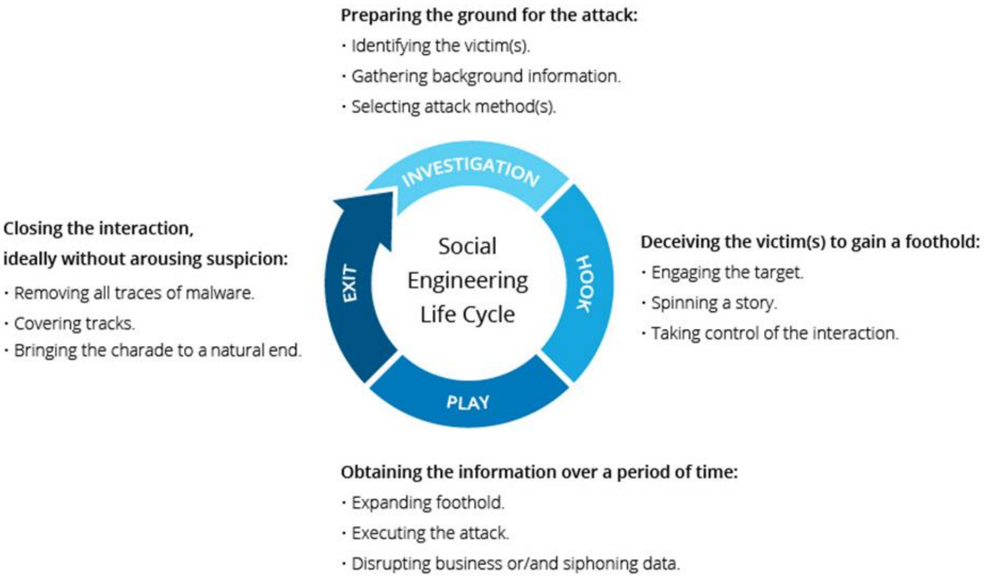
There are several approaches to social engineering attacks that can be used in combination or individual to attack any security system (Krombholzj *et al.*, 2015). A technical approach is one of the approaches implemented in the healthcare sector (Mohan and Singh, 2016). Several breaches causing misrepresentation, tampering of electronic medical records, therefore, have surfaced. Types of threats that are either internal or external pose different forms of hospital information security (Samy, Ahmad, and Ismail, 2010). Of all, power failure of servers or acts of human negligence are potentially avoidable but increase security threats (Samy, Ahmad, and Ismail, 2010).

Physical Approaches

Physical approaches contain information collected through a natural method such as dumpster diving. Attackers might retrieve certain sensitive information by going through garbage, such as notes with passwords, printouts

Jurnal Administrasi Kesehatan Indonesia Volume 8 No 1 June 2020
Published by Universitas Airlangga
Doi:10.20473/jaki.v7i2.2019.132-138

with an address or other hospital's confidential information. Physical approaches can also include physical theft of data or a threat to a person who has access to sensitive health data systems. Healthcare organizations that handle or store confidential health data are always susceptible to security threats and, therefore, are expected to be more vigilant. All sensitive data paperworks revealing patients' identity or income should be securely shredded in a shredder once they are no more useful before disposing of them or handing it to someone who will dispose of it later. Moreover, any signed document, x-rays, prescriptions, or case reports should be stored safely and securely with limited physical access to authorized personnel. Currently, the majority of healthcare organizations have secure paperwork disposal policy, including the use of shredders, separate garbage disposal of confidential paperworks etc.


Preparing the ground for the attack:
· Identifying the victim(s).
· Gathering background information.
· Selecting attack method(s).
INVESTIGATION
Closing the interaction,
ideally without arousing suspicion:
· Removing all traces of malware.
· Covering tracks.
· Bringing the charade to a natural end.
EXIT
Social Engineering Life Cycle
HOOK
Deceiving the victim(s) to gain a foothold:
· Engaging the target.
· Spinning a story.
· Taking control of the interaction.
PLAY
Obtaining the information over a period of time:
· Expanding foothold.
· Executing the attack.
· Disrupting business or/and siphoning data.

Source: Imperva Incapsula (2019)

Figure 1. Life Cycle of Social Engineering.

Figure 1 explains the stages of security threat attacks to understand the entire process of social engineering. Each type and approach mentioned in the paper follow the stepwise process of the cycle. It helps to better understand any security threats in the healthcare sector.

Social Approaches

Hackers or attackers usually try to develop a relationship with potential future victims. They are making one of the most used strategies by attackers as it involves a trust factor. Once people get to know each other, they tend to trust strangers and might speak up specific information like access code to healthcare organization data systems given to a stranger who is unauthorized to get it. For example, a nurse practitioner working in a hospital and having electronic medical record access might provide password credentials in the electronic medical record data system to temporary interns or pretentious patients' family members. In both case scenarios, either the temporary interns or disguised patients' family members might get access and misrepresent or tamper unauthorized electronic confidential medical records of a specific patient. The temporary interns might try to gain nurses' trust by developing friendly terms, helping nurses in reducing their daily workloads. After several days of interaction, nurses who are unaware of the real intentions of hackers (temporary interns and pretentious family members) might provide their hospital data access credentials being asked upon or unknowingly by typing it in front of the hackers. This conventional approach can occur in several settings, such as a hospital setting, insurance companies, government health data offices, or universities working on specific health research by analyzing and collecting patients' confidential health data. Hence, it is very vital to determine and understand whom an authorized person can share their authentication credentials to. Thus in the United States, it is essential to undergo the Health Insurance Portability and Accountability Act (HIPAA) formative training and certification for those who are involved in managing and handling health information. It is critically important to safeguard the confidential medical information of civilians of any countries, and such policies should be enforced to continously maintain health data security.

Technical Approaches

Several social networking websites serve as a reservoir of personal information. Attackers collect such information via several internet resources and tend to attack a victim. A hospital employee might post pictures with background reflecting passwords or other sensitive data in the pictures on social media platforms. The HIPAA, for individuals and professionals who serve as a governing body in the United States, enforces strict policies and rules, including amendment of existing rules for better safeguard of citizen's health information in the United States. It enforces penalty and punishments if rules for the safety of health data are not obeyed (Office for Civil Rights, 2013).

Reverse Social Engineering

It is a type of social engineering in which attackers play helper's roles and do not approach the victim initially. They would create a problem for the victim without knowing and would then contact the victim for offering a helping hand. The victim, on the other side, would take help and provide information like password or personal information or install an application which would hack all the personal data.

Socio-technical Approach

A socio-technical approach is a combination of the social aspect and technical element. An attacker would install malware that may be in a folder or USB drive in which the malware would be labelled by a name that will trap a victim, who will click on the folder infected. A hospital visitor might ask a receptionist to plug in the USB for one or to get entryway into the hospital IT system.

Office Communication

Several internal communications amongst colleagues via email might open the door for attackers using almost similar appearing email addresses, but an employee who is in a rush, will not check the addresses sometimes and end up being a victim. It can involve a physician handling confidential health data of current patients or nurses or others.

Computer-supported Collaboration

Several channels of communication between clients and company employees might open up a potential loophole for the security breach. Several web 2.0 services might also become a tool for hackers.

External Communication

Apart from the internal office communication, several external communications involve blogs and web 2.0 services, which might open a channel for social engineering attacks. There are several types of social engineering attacks (Conteh and Schmick, 2016). The approaches explained previously are the possible platforms or resources used to implement a security threat. While, the types of social engineering attacks provide information about existing practical scenarios and ways in which an attack could occur. The types help to understand how one might be susceptible to security threats while being exposed to any of the approaches mentioned above, like working in hospital offices, being an active user of social media, etc.

Phishing

It is a type of attack in which a message or email would redirect the victim to a legitimate site and would ask personal identification information. The message would reflect a sense of urgency and test a person's excellent knowledge of judgment primarily in the extreme environment of prompted importance.

Baiting

It is similar to phishing, but in this, the attacker lures the victim for providing personal identification information. It can be a gift or free flight tickets for vacation.

Quid pro quo

It is one of the most hybrid versions amongst the rest. The attacker would offer assistance and pretend to be a technical expert when the victim is facing technical issues. The attacker would ask the victim to install a malware in one way or the other.

Tailgating

The attacker would try to get access to a restricted area by following/tailgating a person having access to a restricted area. This is also one type of social engineering in which the attacker pretends to be trustworthy.

Pretexting

The attacker in this scenario uses a preformed well-knit story to trap a victim. The story would require urgent actions and hence leave very little time to the victim to think.

Several cybercrimes occur due to the easy availability of personal data as well as enterprise information on the internet. The majority of social engineering attacks are anonymous, and hence it is difficult to catch the hacker as well as charge them for the crime. This might be the encouraging reason why social engineering, as well as cybercrime, is increasing. Most of the attacks are successful due to the vulnerability of the victim.

Vulnerabilities

Social engineering attacks are never victorious without the potential victim being vulnerable in one way or the other. Hackers would target the psychological aspects of a person after researching thoroughly about them. Vulnerabilities can be anything from using the same password for all applications or access codes wherever required, not considering password security training seriously (Medlin, Cazier and Foulk, 2010). In addition, they were not adequate even though if provided often, willingness to share the password or the updated password with somebody or something and more prolonged or frequent change of password make an individual share the passwords more often (Heartfield, Loukas and Gan, 2016).

Moreover, it is observed that females reflecting neurotic behaviour traits are more vulnerable to responding to phishing emails or visiting the insecure website over other females and males. Overall female users are more susceptible to such attacks over males and play a role in susceptibility in part usage of the internet as well as social media websites. Finally, several traits of being talkative or conversational, open, and positive are more vulnerable to social engineering attacks (Heartfield, Loukas and Gan, 2016).

Hence, taking several susceptibilities of potential victims into consideration might help mitigate the attacks in its developing stage of the attacker's plan. Addressing the vulnerabilities after identifying it at both individual and organizational levels can help to reduce such attacks in healthcare organizations.

Various Settings and Contexts Vulnerable To Social Engineering Attacks

Analyzing vulnerabilities at US hospitals, not just enterprises or big corporates are targeted for such attacks, but more significant health care industries like hospitals are targeted as well for such social engineering attacks (Medlin, Cazier and Foulk, 2010). The reason of targeting healthcare systems is the availability of patients' health information, including their demographics. In certain times, such theft might allow attackers to use somebody's health identity to receive health insurance benefits. It can result in identity theft as well or can lead to heightened insurance charges/fees. Not only the increased insurance rate but also breach into somebody's health data might also make them vulnerable to different types of discrimination from health insurance coverage denial to discrimination in a social and professional environment.

People are more vulnerable to persuasion especially when a higher authority body is demanding specific information (Bullée *et al.*, 2015). A person who is a hacker might act as if they are from a project management office, government auditing body for the hospital, or pretend to be a chief executive officer and demand for specific information on hospital settings. In such a context, people fall preys quickly more because the potential hacker seems to be a legitimate source or might dress up as a reasonable person, maybe a police officer. Hacking into organization's information might lead to loss of some confidential information to rivals, physical damage to data as well as property, loss of clients' information including credit card information, health care sensitive data, which might lead to loss of trust in the organization (Chitrey, Singh and Singh, 2012).

Hacking into the pharmaceutical industry database, which has clinical trial data of ongoing drugs or medical device testing, is another vulnerable setting. Testing of new drugs and medical devices is an essential and continuous process (Patel, 2019). Hence, health care system settings are vulnerable to social engineering attacks. Reverse social engineering attacks on social networks online observe that not only the hospitals and other settings are targeted for social engineering attacks, but also attackers execute reserve social engineering attacks through online social networking services like Facebook, LinkedIn, Friendster's (Irani *et al.*, 2011). Using social networking websites for social engineering attacks is the most effective as the potential victims might consider accepting a friend request of a stranger (attacker), due to several mutual friends or having an attractive profile picture to lure the victim. Once the attacker gains access to all information of the victim, it becomes easy for an attacker to execute a reverse social engineering attack.

Precautionary Steps

Taking measures, including technical and physical security, is not enough for social engineering attacks in healthcare organizations. Since this unique type of hacking attack includes persuasion as well, the first step would be raising awareness about it amongst colleagues, employees, patients, and every single individual working in that healthcare organization. Some might know about it, but emphasizing its importance and risks, if not considered, might end up in a hazardous situation. Educating vulnerable population in healthcare organizations or any settings about it is the most effective way to mitigate such attacks (Smith, Papadaki and Furnell, 2013). Raising awareness through websites or digital storytelling and educating about social engineering attacks, its types, and how to avoid it might also help to mitigate the problem of vulnerability (Patel, 2017). The use of social networking websites like Facebook for revealing personal details as well as information about everything might make a potential victim more vulnerable (Jagatic *et al.*, 2007). Thus, several precautionary measures like establishing a user profile on social networking websites only available to friends, removing the last name, or changing it a bit might make a person less searchable on social networking websites and their directories (Brown *et al.*, 2008). For example, fewer details on social networking websites can be revealed just by giving a new job position update ora small thing like check-ins at someplace or hotels.

Apart from personal training and education, at the organizational-level several frameworks have been already researched and tested. These include authorization, authentication, accounting, sandboxing techniques, developing and implementing strict enterprise policies/laws, monitoring, machine learning, and integrity checking (Heartfield and Loukas, 2015). Evaluating the existing organizational policies could help to better safeguard health information and translate research results of an improved security system to the real-world implementation (Patel, 2018).

CONCLUSION

Understanding types and techniques of social engineering in the first place will help to mitigate the attack attempts in healthcare settings. Keeping oneself updated in terms of evolutionary attacks might also help to avoid being a prey to such attacks and avoid risking patients' health data. Organizational measures are all secondary level steps; one will fail to evaluate if an email, which they just relieved, is a spam email, phishing email, or the website they are clicking is a malware. Keeping it simple is the most effective way to spread information to potential attackers. Not posting information which is accessible to the public would reduce the chances of being vulnerable. Alternatively, training hospital/healthcare employees regarding potential threats to the confidential health data of patients by providing contingency plans might help secure patients' information.

POLICY IMPLICATIONS

Strict workplace policies should be developed for countries that are currently lacking monitoring on safeguarding personal and sensitive health data of their citizens. In order to continue maintaining patient and consumer trust, healthcare organizations and authorities should develop several policies similar to the HIPAA to train every employee who is directly or indirectly involved in the management, collection, analysis and storage of confidential healthcare data related to patients' identity.

CONFLICT OF INTEREST

The authors state that there is no conflict of interest for this article.

REFERENCES

Brown, G. *et al.* (2008) 'Social networks and context-aware spam', in *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, pp. 403–412. doi: 10.1145/1460563.1460628.

Bullée, J. W. H. *et al.* (2015) 'The persuasion and security awareness experiment: reducing the success of social engineering attacks', *Journal of Experimental Criminology*, 11(1), pp. 97–115. doi: 10.1007/s11292-014-9222-7.

Chitrey, A., Singh, D. and Singh, V. (2012) 'A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model', *International Journal of Information and Network Security (IJINS)*, 1(2), p. 45. doi: 10.11591/ijins.v1i2.426.

Conteh, N. Y. and Schmick, P. J. (2016) 'Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks', *International Journal of Advanced Computer Research*, 6(23), pp. 31–38. doi: 10.19101/ijacr.2016.623006.

Heartfield, R. and Loukas, G. (2015) 'A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks', *ACM Computing Surveys*, 48(3), p. 37. doi: 10.1145/2835375.

Heartfield, R., Loukas, G. and Gan, D. (2016) 'You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks', *IEEE Access*, 4, pp. 6910–6928. doi: 10.1109/ACCESS.2016.2616285.

Irani, D. *et al.* (2011) 'Reverse social engineering attacks in online social networks', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 55–74. doi: 10.1007/978-3-642-22424-9_4.

Jagatic, T. N. *et al.* (2007) 'Social phishing', *Communications of the ACM*, 50(10), pp. 94–100. doi: 10.1145/1290958.1290968.

Krombholz, K. *et al.* (2015) 'Advanced social engineering attacks', *Journal of Information Security and Applications*, 22, pp. 113–122. doi: 10.1016/j.jisa.2014.09.005.

Mohan, P and Singh, M 2016, 'Security Policies for Intelligent Health Care Environment', Procedia Computer Science, vol. 92, pp. 161–167.

Medlin, B. D., Cazier, J. A. and Foulk, D. P. (2008) 'Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks: How Many of

Your Employees Would Share Their Password?', *International Journal of Information Security and Privacy (IJISP)*, 2(3), pp. 71–83. doi: 10.4018/jisp.2008070106.

Mick, Stephen S and Shay, P. D. (2014) *Advances in health care organization theory*. 2nd edn. Jossey-Bass.

Narayana Samy, G, Ahmad, R, and Ismail, Z 2010, 'Security threats categories in healthcare information systems', Health Informatics Journal, vol. 16, no. 3, pp. 201–209. OCR 2003, Summary of the hipaa privacy rule: HIPAA Compliance Assistance.

OCR 2013, Summary of the HIPAA Privacy Rule, viewed 12 December 2019, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#>.

Patel, N 2017, 'Modern Technology and Its Use as Storytelling Communication Strategy in Public Health', MOJ Public Health, vol. 6, no. 3, pp. 338–341.

Patel, N 2018, 'Bridging the gap of translation research in public health-from research to real world.', MOJ Public Health, vol. 7, no. 6, pp. 347–349.

Patel, N 2019, 'Why New Drugs, Treatments, and Medical Devices Still Needs to be Tested Clinically Before Making it Available in the Market?', Journal of Neurological Research and Therapy, vol. 3, no. 1, pp. 1–5.

Salahdine, F. and Kaabouch, N. (2019) 'Social Engineering Attacks: A Survey', *Future Internet*, 11(4), p. 89. doi: 10.3390/fi11040089.

Smith, A., Papadaki, M. and Furnell, S. M. (2013) 'Improving awareness of social engineering attacks', in *IFIP Advances in Information and Communication Technology*, pp. 249–256. doi: 10.1007/978-3-642-39377-8_29.