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: 10.20473/jaki.v8i1.2020.56-64

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**
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 most vulnerable to social engineering attacks. It is critical to monitor thefts of hospital data as it contains patients' confidential health information. If leaked, the data can impact patients' social as well as professional lives. The hospital data system includes administrative data, as well as employees' personal information, and if hacked, can lead to identity theft. The current paper discusses the 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 stimulate preventive 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: 5 April 2020***

Social engineering is an extraordinarily complex manipulation performed by hackers to gain unauthorized access to data or systems. It is a well-planned strategy exploiting the trust factor between human beings: people naturally trust a stranger asking for help and are willing to help them. Hackers, on the other hand, seek to benefit from such kindness and abuse it (Salahdine and Kaabouch, 2019).

In today's fast-paced world, every employee in industry, business, or professional organizations becomes more flexible and more susceptible to use personal phones or devices for accessing company's or enterprise's data (Krombholz, Hobel, Huber, and Weippl, 2015). By opening up the options for communication channels like web 2.0 (which includes Facebook and Twitter as well as other internet resources), we are increasing our susceptibility to data theft and security breaches in healthcare settings. Allowing individual hospital/healthcare information to become available in the public domain might pose severe threats to an enterprise from hackers. Several organizational theories, including structural contingency theory and transaction cost theory, describe how technological innovations lead to changes in healthcare organizational structures (Mick and Shay, 2014). Such innovations might include installing a new software program in the hospital database for improved efficiency (like the EPIC system) or buying new technology in general.

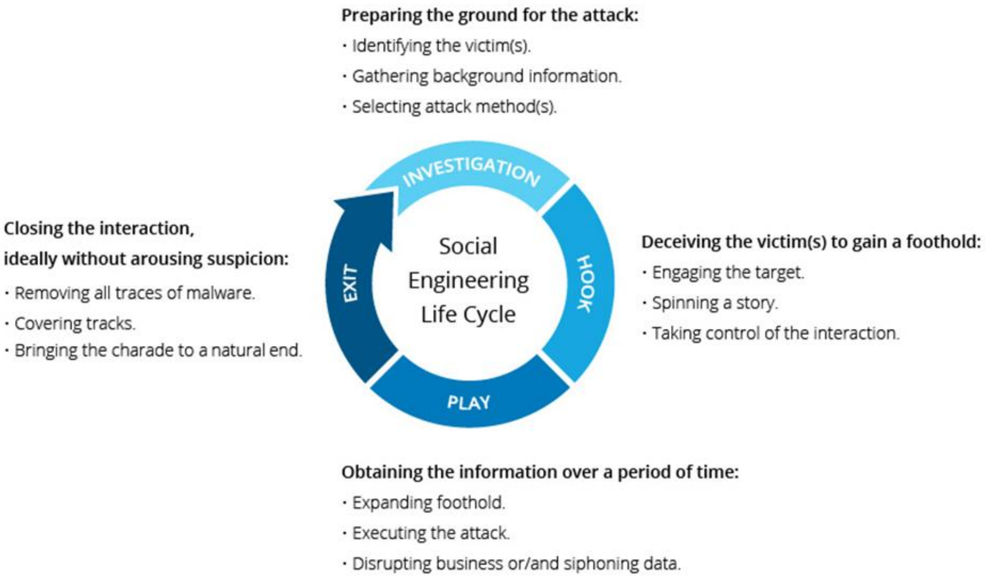
The current paper explores one such aspect of healthcare organizations: hospital information system security. Many studies have talked about information security and its essentiality for different corporate business settings or government institutions, but less focus has been given to hospital information 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 that needs attention in the healthcare sector. This sector includes the pharmaceutical industry, hospitals, health insurance companies, private and government-funded dental clinics, and general health clinics that have sensitive patient health information. It is vital to understand the different types of social engineering attacks, as well as possible vulnerabilities in less-researched fields of healthcare where patients' private information is most prone to identity theft and tampering (Conteh and Schmick, 2016). Globally, the field of information security has advanced from simply installing antivirus software to proactively training employees and increasing awareness regarding susceptibility to and forms of social engineering attacks. Governmental bodies have also set specific standards with penalties if patients' information data is left unprotected and subsequently breached. However, as hackers' resources and types of social engineering attacks continuously evolve, it becomes essential to understand the different types of social engineering attacks and their sources. The objective of the current paper is to address these questions. It further discusses different healthcare settings that are potentially susceptible to the theft of patients' health data and provides possible solutions.

Approaches and types

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

Physical approaches

Physical approaches obtain information collected through a physical method such as dumpster diving. Attackers might retrieve sensitive information, such as notes with passwords, printouts with an address or other hospital-confidential information, by going through garbage. Physical approaches can also include physical theft of data or threatening 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 are therefore expected to be more vigilant. All sensitive paperwork revealing patient identity or income ought to be securely shredded and disposed of or else handed to someone who will dispose of it later. Moreover, any signed documents, x-rays, prescriptions, or case reports should be stored safely and securely with physical access limited to authorized personnel. Currently, the majority of healthcare organizations have a secure paperwork disposal policy, including the use of shredders, separate garbage disposal of confidential paperwork, etc.


Preparing the ground for the attack:
· Identifying the victim(s).
· Gathering background information.
· Selecting attack method(s).
INVESTIGATION
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.
EXIT
Closing the interaction, ideally without arousing suspicion:
· Removing all traces of malware.
· Covering tracks.
· Bringing the charade to a natural end.

Source: Imperva Incapsula (2019)

Figure 1. Life cycle of social engineering.

Figure 1 exhibits the stages of security threat attacks to help 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. This is one of the most popular strategies as it involves a trust factor. Once people get to know each other, they might relay specific information such as access codes to healthcare organization data systems and thereby give it to a stranger who is actually unauthorized to receive it. For example, a nurse practitioner having electronic medical record access working in a hospital might provide password credentials to temporary interns or fake patient family members. In both scenarios, either the temporary interns or the disguised family members might get access and misrepresent or tamper with unauthorized electronic confidential medical records of a specific patient. The temporary interns might also try to gain nurses’ trust by developing friendships and helping nurses reduce their daily workload. After several days of interaction, nurses who are unaware of the real intentions of the hackers might provide their data-access credentials upon either being asked or by unknowingly typing it in front of the hackers. This conventional approach can occur in several settings, such as hospitals, insurance companies, government health data offices, or universities analyzing and collecting patients' confidential health data as part of a research project. Hence, it is vital to determine and understand whom an authorized person can share their authentication credentials with. Thus, in the United States, it is essential for those who are involved in managing and handling health information to undergo formative training and certification under the Health Insurance Portability and Accountability Act (HIPAA). Also, to continually maintain health data security, it is critically important to safeguard confidential medical information of civilians from any country, and such policies should be enforced.

Technical approaches

Several social networking websites serve as a reservoir of personal information. Attackers collect such information via a number of internet resources 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 enforces strict policies and rules for individuals and professionals who serve on governing bodies in the United States, including the amendment of existing rules for better safeguarding of citizens' health information. It also enforces penalties and punishments if rules for the safety of health data are not obeyed (Office for Civil Rights, 2013).

Reverse social engineering approaches

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

Socio-technical approaches

A socio-technical approach is a combination of the social aspect and technical element. An attacker would generate malware in a folder or USB drive labeled with a name that will trick the victim into clicking it. A hospital visitor might ask a receptionist to plug in the USB to gain entry into the hospital IT system.

Office communication approaches

Internal communications amongst colleagues via email might open the door for attackers using similar-appearing email addresses, as an employee who is in a rush might not check the exact addresses and end up becoming a victim. It can involve a physician handling confidential health data of current patients or nurses or others.

Computer-supported collaboration approaches

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 approaches

Apart from internal office emails, several external communications involve blogs and web 2.0 services which might open a channel for several types of social engineering attacks (Conteh and Schmick, 2016). The approaches explained previously are possible platforms or resources used to implement a security threat. The types of social engineering attacks provide information about existing practical scenarios and ways in which an attack could occur. Understanding the types allows one to see 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 approaches

This is a type of attack in which a message or email would redirect the victim to a legitimate-appearing site and would ask for personal identification information. The message would reflect a sense of urgency and test an individual's excellent knowledge in judging information in the extreme environment.

Baiting approaches

This is similar to phishing, but the attacker lures the victim into providing personal identification information by offering a gift or free flight tickets for a vacation.

Quid pro quo approaches

This is a hybrid version of the others. 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 malware in one way or the other.

Tailgating approaches

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

Pretexting approaches

The attacker in this scenario uses a well-rehearsed story to trick the victim. The story would require urgent action and leave little time for the victim to think.

Many cybercrimes occur because of 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 and charge them for the crime. This might be the underlying 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 successful unless the potential victim is vulnerable in one way or another. Hackers often target a person's psychological weaknesses after researching the person thoroughly. Vulnerabilities can be anything from using the same password or access codes for all applications, or not taking password security training seriously enough (Medlin, Cazier and Foulk, 2010). Other situations could include passwords being simply inadequate (even if changed sufficiently often) or someone being willing to share an updated password with somebody. In fact, researchers found that more frequent changes of passwords made an individual more likely to share passwords (Heartfield, Loukas and Gan, 2016).

Moreover, it has been observed that females exhibiting neurotic behavior are more vulnerable than other females and males in terms of responding to phishing emails or visiting insecure websites. Overall female users are more susceptible to such attacks than males. Finally, the traits of being talkative, conversational, open, and positive can make someone more vulnerable to social engineering attacks (Heartfield, Loukas and Gan, 2016).

Hence, taking the susceptibilities of potential victims into consideration can help attackers to formulate the attacks in their developmental stage. Identifying and addressing the vulnerabilities at both individual and organizational levels can help to reduce such attacks in healthcare organizations.

Settings and contexts vulnerable to social engineering attacks

It is not just enterprises or big corporations that are targeted for such social engineering attacks but also healthcare industries like hospitals (Medlin, Cazier and Foulk, 2010). The reason for targeting healthcare systems is the availability of patients' health information, including their demographics. Certain thefts might allow attackers to use somebody's health identity to receive health insurance benefits. It can lead to general identity theft or heightened insurance charges/fees. Breaches of personal health data might also make someone 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 it is a higher authority body that is demanding information (Bullée *et al.*, 2015). A person who is a hacker might act as if they are from a project management office or a government body auditing the hospital; they might pretend to be a chief executive officer and demand specific information about hospital settings. In such a context, people often fall prey more quickly because the potential hacker seems to be a legitimate source or might dress up as a credible person, such as a police officer. A hack into an organization's information might lead to a loss of confidential information to rivals, physical damage to data and property, loss of clients' information including credit card information or healthcare sensitive data, and might lead to a loss of trust in the organization (Chitrey, Singh and Singh, 2012).

A hack into a pharmaceutical industry database containing clinical trial data for ongoing drugs or other medical device testing is another example of a vulnerability. Testing of new drugs and medical devices is an essential and continuous process (Patel, 2019). Hence, healthcare system settings are vulnerable to social engineering attacks. Reverse social engineering attacks on social networks online show that not only are hospitals and other settings targeted for social engineering attacks but attackers also execute reverse social engineering attacks through online social networking services like Facebook, LinkedIn, and Friendster (Irani *et al.*, 2011). Using social networking websites for social engineering attacks is effective since potential victims might consider accepting a friend request from a stranger (attacker), perhaps through several mutual friends or having an attractive profile picture to lure the victim. Once the attacker gains access to information about the victim, it becomes easy for an attacker to execute a reverse social engineering attack.

Precautionary Steps

Technical and physical security measures are not enough to prevent social engineering attacks in healthcare organizations. Since this unique type of hacking attack centers on persuasion, the first step should be raising awareness amongst colleagues, employees, patients, and every single individual working in that healthcare organization. While some people might already have some awareness of the topic, unless the importance and risks are emphasized, the organization might end up in a hazardous situation. Educating a vulnerable population in healthcare organizations is the most effective way to mitigate such attacks (Smith, Papadaki and Furnell, 2013). Using websites or digital storytelling and educating to raise awareness of social engineering attacks and how to avoid them might also help to mitigate the problem of vulnerability (Patel, 2017). The widespread limitation of social networking websites like Facebook for revealing personal details might make a potential victim more vulnerable (Jagatic *et al.*, 2007). Thus, simple precautionary measures, such as establishing a user profile only visible to friends, changing the last name slightly or removing it altogether, might make a person less searchable on social networking websites and their directories (Brown *et al.*, 2008). For example, revealing fewer details on social networking websites about a new job position or checking in at hotels.

Apart from personal training and education, at the organization-level several frameworks have already been 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 existing organization policies could help to safeguard health information better and translate research results of an improved security system into real-world implementations (Patel, 2018).

CONCLUSION

Understanding the types and techniques used in social engineering in the first place will help to mitigate attack attempts in healthcare settings. Keeping updated regarding evolutionary attacks might also help to avoid falling prey to such attacks and avoid risking patients' health data. Organizational measures are all secondary level steps, however, since it is down to individuals to evaluate a spam email, phishing email, or whether the website they are clicking contains malware. Keeping it simple is the most effective way to avoid spreading information to potential attackers. Not posting information in the public domain reduces the chances of being vulnerable. Alternatively, training hospital/healthcare employees about potential threats to the confidential health data of patients and providing contingency plans might help secure patients' information.

Strict workplace policies should be developed for countries that currently lack monitoring on the safeguarding of the personal and sensitive health data of their citizens. In order to continue maintaining patient and consumer trust, healthcare organizations and authorities should develop 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*. San Diego. 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, 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), pp. 45–53. 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), pp. 1–37. 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*. doi: 10.1109/ACCESS.2016.2616285.

Irani, D. *et al.* (2011) ‘Reverse social engineering attacks in online social networks’, in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Amsterdam: Springer-Verlag Berlin Heidelberg. 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.

Medlin, B. D., Cazier, J. A. and Foulk, D. P. (2010) ‘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). doi: 10.4018/jisp.2008070106.

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

Mohan, P. and Singh, M. (2016) ‘Security Policies for Intelligent Health Care Environment’, *Procedia Computer Science*, 92, pp. 161–167. doi: 10.1016/j.procs.2016.07.341.

Narayana Samy, G., Ahmad, R. and Ismail, Z. (2010) ‘Security threats categories in healthcare information systems’, *Health Informatics Journal*, 16(3), pp. 201–209. doi: 10.1177/1460458210377468.

Office for Civil Rights (OCR) (2013) *Summary of the HIPAA Privacy Rule*, *Health Information Privacy*. Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html# (Accessed: 12 December 2019).

Patel, N. (2017) ‘Modern Technology and Its Use as Storytelling Communication Strategy in Public Health’, *MOJ Public Health*, 6(3), pp. 338–341. doi: 10.15406/mojph.2017.06.00171.

Patel, N. (2018) ‘Bridging the gap of translation research in public health-from research to real world.’, *MOJ Public Health*, 7(6), pp. 347–349. Available at: https://www.researchgate.net/profile/Naiya_Patel2/publication/329451197_Bridging_the_gap_of_translation_research_in_public_health_-_from_research_to_real_world/links/5c094a694585157ac1ad2309/Bridgi ng-the-gap-of-translation-research-in-public-health-from-r.

Patel, N. (2019) ‘Why New Drugs, Treatments, and Medical Devices Still Needs to be Tested Clinically Before Making it Available in the Market? A Systematic Review’, *Journal of Neurological Research and Therapy*, 3(1), pp. 1–5. doi: 10.14302/issn.2470-5020.jnrt-19-2618.

Salahdine, F. and Kaabouch, N. (2019) ‘Social Engineering Attacks: A Survey’, *Future Internet*, 11(89), pp. 1–17. doi: 10.3390/fi11040089.

Smith, A., Papadaki, M. and Furnell, S. M. (2009) ‘Improving awareness of social engineering attacks’, in *IFIP Advances in Information and Communication Technology*. Brazil: Springer, pp. 249–256. doi: 10.1007/978-3-642-39377-8_29.