Coping with Changing Contexts: A Healthcare Security Perspective

Naqvi Bilal, Ardito Carmelo

DOI: 10.1007/978-3-030-98388-8_13

Coping with Changing Contexts: A Healthcare Security Perspective

Bilal Naqvi[1] (✉) [0000-0001-5271-5604] and Carmelo Ardito[2]

[1] LUT Software, LENS, LUT University, Lappeenranta 53850, Finland
[2]Dipartimento di Ingegneria Elettrica e dell'Informazione (DEI), Politecnico di Bari, Bari, Italy
syed.naqvi@lut.fi

Abstract. With the fourth industrial revolution, there is a digitization wave going on for the transformation of existing systems into modern digital systems. This has opened the window for many opportunities, but at the same time, there is a multitude of cyber-security threats that need to be addressed. This paper considers one such threat posed by phishing and ransomware attacks to the healthcare infrastructures. Phishing has also been the most prevalent attack mechanism on the healthcare infrastructures during the ongoing COVID-19 pandemic. The paper proposes two intervention strategies as a step towards catering to the challenges posed by phishing and ransomware attacks in the context of healthcare infrastructures.

Keywords: healthcare, phishing, ransomware, security, usability, usable security

1 Introduction

The fourth industrial revolution (referred to as Industry 4.0) involves automation of the existing infrastructures and brings in many opportunities and avenues for digitization of existing mechanisms including healthcare. From a healthcare perspective, some of these avenues include the use of telemedicine, artificial intelligence (AI)-enabled medical devices for scanning and procedures, blockchain-based health records, among others [1]. Although each of these avenues refers to limitless opportunities for improvements, yet several challenges emerge and are imperative to be addressed. One such challenge is the consideration of human factors associated with the deployment of these digitized solutions.

Human factors are about considering human abilities, limitations, and characteristics in the design of tools, devices, systems, and services. One prevalent mechanism aimed at exploiting the human limitation of distinguishing between original and fake content is known as phishing [2]. Phishing occurs when the attacker persuades the victim into doing something which is not beneficial for the victim or the system. Prevalent ways to initiate phishing include emails, advertisements, among others. With increased phishing, there have been instances of phishing attacks ultimately taking the form of ransomware attacks, where the attacker encrypts the systems' files and asks for money to decrypt them. The implications of such attacks in healthcare infrastructures are not limited to monetary losses, but there are risks including (but not limited to) safety of patients, breach of the privacy of the medical records, etc. The recent trends show that phishing attacks are used as a common vector for launching ransomware attacks. Some of the recent incidents include:

1. Various malicious emails attempting to spread ransomware to several individuals were identified. The target was a Canadian government health organization actively engaged in the COVID-19 pandemic response efforts, as well as a Canadian university that is conducting COVID-19 research[1].
2. Hackers broke into computers at Hammersmith Medicines Research, a London-based company that was carrying out clinical trials for new medicines against the COVID-19 pandemic. The hackers then asked for ransom to let the professionals use their systems[2].

The case considered in this paper has relevance with the ongoing COVID-19 pandemic since the two incidents just discussed have occurred recently. However, this problem existed before COVID-19 and has ramifications even after. For instance, a ransomware attack on Victorian Regional Hospitals in Australia, where successful phishing led to ransomware on patient health care records[3]. Many surgeries were delayed due to the non-availability of the records. Furthermore, Europol, the European Union (EU) law enforcement agency has received reports of intensifying cyber-attacks in almost all its 27 member countries. The ransomware attacks come amid an increase in other cyber-attacks related to the pandemic. They have included a rash of "phishing" emails that attempt to use the crisis to persuade people to click on links that download malware or ransomware onto their computers.

This paper considers the challenges posed by phishing and ransomware attacks to the healthcare personnel and infrastructures and aims to shed light on the following research question:

RQ: *How to cope with changing contexts while considering the threats posed by phishing and ransomware attacks in the context of healthcare infrastructures?*

To answer this question, this position paper presents two intervention strategies, (1) educational intervention, and (2) design intervention. The remainder of the paper is organized as follows. Section 2 presents and background. Section 3 presents the intervention strategies to cater to the changing context, and Section 4 concludes the paper.

2 Background

The state of the art concerning digitization in healthcare shows that the industry has to do a lot to catch up to the pace of Industry 4.0. For instance, survey results [1] show

[1] https://blog.malwarebytes.com/cybercrime/2020/10/fake-covid-19-survey-hides-ransomware-in-canadian-university-attack/

[2] https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

[3] https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0

that seven percent of healthcare and pharmaceutical companies have gone digital as compared to 15 percent of companies in other industries, however, the ongoing COVID-19 pandemic has increased the pace of digitization of the healthcare industry. The results also identify seven key trends of digital transformation in healthcare in 2021. One of the trends is the rise in on-demand healthcare. Consumers are interested in healthcare services at a time of their convenience. It also identifies that the consumers use online means for finding doctors (47%), searching medical facilities (38%), and booking a medical appointment (77%). Furthermore, some other trends of digital transformation in healthcare include the use of big data and predictive analysis, the use of virtual reality for treating patients, use of wearable medical devices, among others [1]. These numbers identify both threats and opportunities. Opportunities could include, for example, the development of human-centric procedures, incorporating the elements of the UX in the systems and services, considering different age groups and impairments in the interface design; however, there is a multitude of threats, which could hamper all the merits of technology and digitization. Cyber-gangs and attackers have increasingly been using phishing and other attacks to cause damage to the existing healthcare systems and services and generate money using this means. Having said that, the focus needs to be not only on the development and deployment to keep up the pace with Industry 4.0 but also on contextual aspects and the human factors associated with these solutions.

From a healthcare perspective discussed in this paper, phishing is a common threat faced by healthcare personnel and a major cyber-security risk for healthcare infrastructures. A study was conducted in the United States to assess the anti-phishing preparedness of 5416 healthcare staff [3]. The participants of the study were sent 20 emails during the study. The results reveal that 65.3% of the participants clicked at least 2 phishing emails, with 772 participants clicking at least 5 emails. In another study [4], analysis of around 143 million Internet transactions revealed that 5 million among those were suspected phishing threats.

With such numbers and phishing attacks among the most prevalent vectors for launching ransomware attacks, it is vital to discuss and formulate intervention strategies to cater to this challenge. Ransomware is a type of malware designed to extort money from victims, who are prevented from accessing their systems [5]. The two most prevalent types of ransomware are encryptors and screen lockers. Encryptors, as the name implies, encrypt data on a system, making the content useless without the decryption key. Screen lockers, on the other hand, simply block access to the system with a "lock" screen, asserting that the system is encrypted.

One other aspect which needs to be considered is that while many of the healthcare organizations are adopting electronic means for patient records and other digital systems, the healthcare personnel seem to have limited awareness of the cyber-security threats. Moreover, most of the IT training content for healthcare staff is focused on how to use the software and applications, not the cyber-security attacks they could be exposed to. It is, therefore, pertinent to consider approaches to protect against cyber-security threats induced due to this evolving technological infrastructure. However, for this paper, we will limit to addressing the challenges posed by phishing and ransomware to the healthcare infrastructures.

3 How to cope with challenges in the changing context?

Having discussed the need for and importance of coping with the challenges posed by phishing and ransomware attacks, this section presents the intervention strategies to cope with these challenges. Broadly the intervention strategies can be classified into 2 categories:

1. Educational intervention strategies
2. Design intervention strategies

3.1 Educational intervention strategy

This strategy aims at educating the users of the system to be able to protect themselves against phishing and ransomware attacks. Three elements form the core of this intervention this strategy [13]:

- *Awareness*: the aim here is to catch people's attention and convince them that cyber security is worth their attention.
- *Education*: once people are aware and willing to learn, specialized information could be provided which helps to improve the security behavior and assists people to develop accurate mental models about cyber-security. To educate users, both traditional modes of education (i.e., conducting specialized courses) [14], and the use of gamification techniques have been proposed [15].
- *Training*: It is more specific and helps people to acquire skills, for instance, how to identify and report a phishing attack? It is relevant to consider the user's role in a system while planning and conducting such training, and thus requires preparation of the training manuals accordingly.

The following two approaches in line with the core elements just discussed are worth considering to support the educational intervention strategy.

Training and supporting developers at work.

Human factors and cyber-security have evolved as two different domains [7]. Expertise in both these domains (human factors and security) is hard to find in one person [8,9], therefore, developers don't often consider the fact that the security systems and services without consideration of human factors despite being secure against known vulnerabilities could still be susceptible to users' mistakes leading to a breach. Therefore, there is a need for providing training on usability and usable security both at the educational institutions and work [10]. Such activities are expected to help the developers in understanding the unusable security mechanisms and realize that despite being secure against various attacks the systems will still be susceptible to user mistakes leading to malicious compromises.

Furthermore, design patterns can be effective to support the developers in handling security and usability issues [11]. Patterns can support the developers in assessing the usability of their security options, and vice versa. Each pattern expresses a relation between three things, context, problem, and solution. Patterns provide real solutions, not abstract principles by explicitly mentioning the context and problem and summarizing the rationale for their effectiveness. Since the patterns provide a generic "core" solution, its use can vary from one implementation to another. A usable security pattern encapsulates information such as name, classification, prologue, problem statement, the context of use, solution, and discussion on the right use of the pattern. Naqvi and Seffah [11] present more details on how a usable security pattern looks like. A challenge in this regard is collecting such patterns and making a catalog to be disseminated among the developers.

Training the developers and supporting them at work with the use of design patterns can assist in the development of user-centric security solutions that consider attributes of systems' users such as literacy and aptitudes, and thus are less likely to be susceptible to users' mistakes leading to security breaches.

Initiating cross-disciplinary education and training mechanisms.

Another approach that could be adopted is initiating a cross-disciplinary forum to create educational content and new knowledge material. This forum can also be seen as a supportive mechanism for conducting usable security training for developers. Such a forum would include human factors and cyber-security researchers, and industry practitioners (see Fig.1). The forum would exchange and understand viewpoints from academia and industry perspectives and identify the challenges that arise. The challenges are then assessed in a workshop/hackathon for identification of the new solutions. The solutions are then documented to create training manuals for the stakeholders. The two benefits of such a forum are:

1. A means for usable security knowledge sharing and dissemination between industry and academia. This would help in addressing the inconsistencies in perceptions between industry and academia about human factors in security.
2. A bidirectional mechanism in which the state of the art in research is closely connected with challenges and practices in the industry.

Other participants for this forum could include junior researchers, junior developers, and representatives from vocational training institutions. From the educational intervention perspective, the outcomes of the forum could be used for educating the participants such as:

- *junior researchers*, for advancing their research on the topic and trying to come up with solutions that address industry needs thereby creating an avenue for industry-academia collaboration;
- *junior developers*, for training purposes and addressing the multidisciplinary challenge posed by usable security. The outcomes could also be documented as design patterns for the developers to apply in specific contexts; and
- *vocational training institutions*, have a wider outreach in the society. They can use outcomes of the forum to create new courses and content focused on the training of health care personnel, senior students, and common citizens.

Furthermore, new content addressing the challenges can also be used in conventional educational activities such as at schools and colleges.

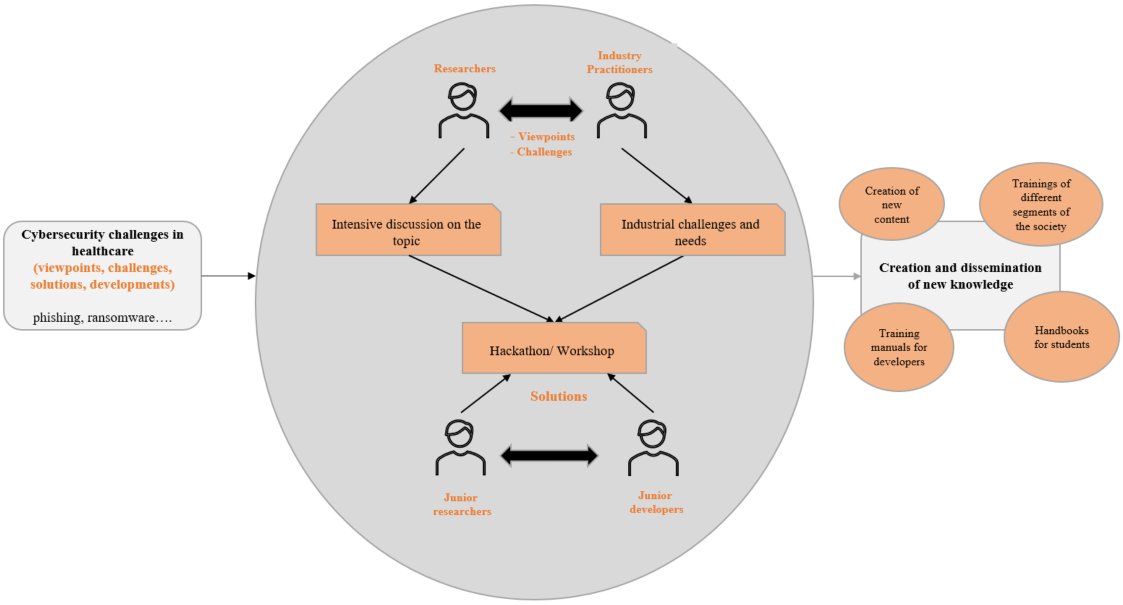
Cybersecurity challenges in healthcare
(viewpoints, challenges, solutions, developments)
phishing, ransomware….
Researchers
Industry Practitioners
- Viewpoints
- Challenges
Intensive discussion on the topic
Industrial challenges and needs
Hackathon/ Workshop
Solutions
Junior researchers
Junior developers
Creation of new content
Trainings of different segments of the society
Creation and dissemination of new knowledge
Training manuals for developers
Handbooks for students

Fig. 1. Sequence of activities for initiating cross-disciplinary education and training mechanisms

One vital consideration while planning for initiating a cross-disciplinary education and training mechanism is to avoid creating silos. Thorough consideration needs to be put in for identifying similar forums and hackathons to synthesize their findings into a set of collective findings addressing the issue; such a synthesis could itself be very challenging especially in the case of domain-specific recommendations.

3.2 Design intervention strategy

This strategy refers to design choices that aim to support and guide users in developing accurate mental models concerning cyber-security. This involves the use of visual elements, color codes, highlights, among other visual techniques to supports user's decision-making abilities [16]. In the context of phishing attacks, it could also take the form of a tool that generates caution in case of a suspicious email and can be integrated with the email applications.

Furthermore, to facilitate the users in detecting and avoiding phishing attacks, existing HCI methods need to be considered, for instance, the use of task models for modeling interactions and identifying all possible scenarios that could lead to a successful phishing attack. One relevant approach here is the use of a polymorphic user interface to warn the users (healthcare personnel) against phishing. Aneke et al., [12] propose such a scheme, which addresses three main goals, (1) prevent user habituation, (2) provide an explanation of the attack, and (3) educate the user on cyber-attacks and risks.

In addition, the prototype shows three panels to explain why a URL could be fake. However, there is a need to identify such implementations and work for their deployment after carefully analyzing any room for improvements.

4 Conclusion

In the era where the development is driven mainly to keep up the pace with Industry 4.0, this paper discusses an important challenge posed by phishing and ransomware attacks considering the case of healthcare personnel and infrastructures. The topic discussed in the paper is timely and important.

The paper advocates that there is a need to go beyond the traditional ways of development and adopt a multi-faceted approach for addressing the challenges posed by rapidly changing contexts. The paper proposes two strategies that need to be considered to cater to the challenges we face. Although we consider the healthcare perspective in this paper, the proposed strategies hold equally good for other domains. The educational intervention strategy aims at role-based educational activities, we also propose a cross-disciplinary forum for discussion of issues involving human factors in security, preparation of training manuals, and educational content. Moreover, the design intervention strategy aims at incorporating elements of human-computer interaction in the design of security systems and services. We believe that these strategies have the potential of contributing towards improvement in the state of the art, however, refinement to strengthen and improve these strategies would be considered as part of ongoing work on the topic.

References

1. M. Reddy.: Digital Transformation in Healthcare in 2021: 7 Key Trends. Available at: https://www.digitalauthority.me/resources/state-of-digital-transformation-healthcare/ (2021)
2. Hong, J. The state of phishing attacks. Communications of the ACM 55(1). pp.74-81 (2012).
3. Gordon, W.J., Wright, A., Glynn, R.J., Kadakia, J., Mazzone, C., Leinbach, E., Landman, A. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. Journal of the American Medical Informatics Association 26(6), pp. 547–552 (2019).
4. Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. Phishing in healthcare organizations: threats, mitigation, and approaches. BMJ health & care informatics 26(1). E10031 (2019).
5. Cartwright, E., Castro, J.H., Cartwright, A., To pay or not: game theoretic models of ransomware. Journal of Cybersecurity 5(1), pp. 1-12 (2019).
6. HealthIT.gov. What are the advantages of electronic health records? Available: https://www.healthit.gov/faq/what-are-advantages-electronic-health-records (2019).
7. Garfinkel, S., Lipford, H.R.: Usable Security History, Themes, and Challenges. Morgan and Claypool, USA (2014).
8. Naqvi, B., Clarke, N., and Porras, J. Incorporating the human facet of security in developing systems and services. Information and Computer Security 29(1), pp. 49-72. (2021).

9. Naqvi, B., Porras, J., Oyedeji, S. and Ullah, M. Towards identification of patterns aligning security and usability. In: Abdelnour Nocera, J. et al., eds. Beyond Interactions: INTERACT 2019 IFIP TC 13 Workshops, Paphos, Cyprus, September 2–6, 2019, Revised Selected Papers. Lecture Notes in Computer Science. Vol. 11930. Cham: Springer, pp. 121–132. (2020).
10. Caputo, D.D., Pfleeger, S. L., Sasse, M. A., Ammann, P., Offutt, J., and Deng, L.: Barriers to Usable Security? Three Organizational Case Studies. IEEE Security Privacy 14(5), pp. 22–32, (2016).
11. Naqvi, B., Seffah, A.: Interdependencies, Conflicts, and Trade-offs between Security and Usability: Why and how should we Engineer Them?. In: 1st International Conference, HCI-CPT 2019 Held as Part of the 21st HCI International Conference, HCII 2019 Orlando, FL, USA, pp. 314-324, (2019).
12. Aneke, J., Ardito, C., Desolda, G. Designing an Intelligent User Interface for preventing phishing attacks. In: Abdelnour Nocera, J. et al., eds. Beyond Interactions: INTERACT 2019 IFIP TC 13 Workshops, Paphos, Cyprus, September 2–6, 2019, Revised Selected Papers. Lecture Notes in Computer Science. Vol. 11930. Cham: Springer, pp. 121–132. (2020).
13. Sasse, A., Rashid, A.: The Cyber Security Body of Knowledge - Human factors knowledge area v 1.0. University of Bristol, Available at: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf (2019).
14. Turner, C.F., Taylor, B., Kaza, S.: Security in Computer Literacy- A Model for Design, Dissemination, and Assessment. In: Proceedings of the 42nd ACM technical symposium on Computer science education, Dallas, Texas, USA, pp. 15-20, (2011).
15. Yang, C.C., Tseng, S.S., Lee, T.J., Weng, J.F., Chen, K.: Building an Anti-Phishing Game to Enhance Network Security Learning. In: 12th IEEE International Conference on Advance Learning Technologies, pp. 121-123, (2012).
16. Franz, A., Zimmerman, V., Albrecht, G., Hartwig, K., Reuter, C., Benlian, A., Vogt., J.: SoK: Still Plenty of Phish in the Sea—A Taxonomy of User-Oriented Phishing Interventions and Avenues for Future Research. In: USENIX Symposium on Usable Privacy and Security (SOUPS), Virtual Conference, pp. 339-357, (2021).