Editorial article

Journal of Sensor Networks and Data Communications

Network Security and Privacy in Social Work

Fahri Özsungur

Adana Science and Technology University

*Corresponding author
Fahri Özsungur, Adana Science and Technology University

Submitted:14 Oct 2020; **Accepted:** 19 Oct 2020; **Published:** 29 Oct 2020

Abstract
This study aims to reveal the importance of network security and privacy in social work and to determine the risk status of the beneficiaries and the institution in this context. Network security and privacy are important in the functions of social work to increase the social welfare of the elderly, women, children, and disabled people, to increase their active participation in the life and to ensure their integration into society. The strategies to be formed by social work institutions in this regard will ensure the safety of the beneficiaries and prevent possible support losses. In this context, possible risk elements and levels should be determined, and the measures should be taken into account in the corporate strategy.

Introduction

Social work has important functions in terms of eliminating the deficiencies of individuals due to declines, reintegration into society, adaptation to the environment, and post-retirement services [1,2]. Relationships between individuals in the society are improved and developed through social work via the ministry of family and social policies, the ministry of health, the ministry of national education, and similar institutions [3-5]. Policies related to many issues such as autism spectrum patients, the disabled and elderly people, orphans, women, family, culture, occupational health and safety, social security, and work-life are developed through social work [6-9].

In the institutional context, the function of social work on individuals of society requires minimizing the risks that may arise from some security vulnerabilities in today's technology [10,11]. Networks in which individuals' personal data are circulated carry a significant risk of security vulnerability [12,13]. People who want to take advantage of the physical, mental, psychological, and social decline of elderly people can use these networks for fraud [14]. Elderly people who have no income other than wages after retirement are at great risk through this fraud. The need for masks and needles that arise with the pandemic can cause individuals to fraud through e-mails.

One of today's cyber threats is social media. Individuals share their personal information publicly through social media [15]. Some pictures, messages, and personal information about women's private lives can be seized by fraudsters. In addition, it is necessary to protect children's personal information due to the sexual abuse of children, custody/parental problems, risk of kidnapping. Therefore, network security is important.

In social work, the network is important in terms of functionality that emerges with digitalization. The network provides care of the elderly, monitoring their illnesses, improving their social lives, controlling risks, managing financial transactions, and meeting their daily needs.

Social Work Personnel Based Measures

High-security authentication systems such as fingerprints or retina scanning should be implemented for the security of the social work staff network [16]. Attention should be paid to the security level of identity verification in the storage of computers, digital devices, and data in public institutions and organizations where social work is carried out. In particular, information about the past in the adoption of children, information that will enable the determination of the location of women victims of violence by third parties, and personal information regarding salary payments in social security should be protected by special network firewall applications [17]. Not every staff member should have access to this information.

For network security, the identity queries of the personnel should also be applied in network traffic [18]. Multi-factor authentication can be recommended in this context. Special authorizations, job descriptions, network monitoring should be applied strategically to accessing the network. It is necessary to determine the identity (ID) while distributing the authority of the network according to the personnel in charge [19]. However, network users should not be able to track the administrator ID that monitors the network.

It can be envisaged that the inputs of the personnel from digital devices such as smartphones and Ipads are restricted for some data. Because the access to a third device to the system creates a second risk. For this reason, personal information of social work beneficiaries should be divided into risk groups according to their importance.

Table 1: Risk levels in social work

Beneficiary / institution	Information	Risk level
Beneficiary information	Demographic information (age, ID number, date of birth, etc.), medication information, social security number Bank account information, address and contact information Digital usernames and passwords Photos, emails, digital messages, social media posts	High risk High risk High risk High risk
Information on the institution	Social work personnel demographic information, usernames, and passwords Social work institution confidential information Institutional photos, e-mails Social work staff job location information Corporate announcements, news	High risk High risk High risk Moderate risk Moderate risk
Beneficiary information	Health information, disability status	Moderate risk
Information on the institution	Social work corporate mission and vision, public information Public address and contact information of the institution	Low risk Low risk
Beneficiary information	Hobbies, publicly shared political views, public social activities	Low risk

External Security Measures

Alternative network protection systems such as honeypots, intrusion prevention systems, anti-virus software can be useful for external security [20,21]. However, what is important is that the system in which information is stored against a possible cyberattack has been backed up [22]. In addition to the breach of data privacy, the access problem is important. Problems encountered in accessing social work beneficiaries 'information may negatively affect individuals' lives socially and financially. On the other hand, attacks that will negatively affect the functions of digital devices create new problems related to treatment and care.

Violation of confidentiality can adversely affect the social life and psychology of the institutions and beneficiaries. Deciphering the address or communication information of women victims of violence may lead to the continuation of physical and psychological violence. The seizure of the bank account numbers, phones, or ID numbers of the elderly as a result of a cyber-attack can lead to fraud in salary and bank accounts. On the other hand, hacker access to web-based systems of social work institutions and security vulnerabilities in the network may cause the beneficiaries to be deprived of possible support. In addition, potential risks associated with Network Security and Privacy compromise trust in social work.

Network Security and Privacy Awareness in Social Work

Social work provides multi-faceted contributions by addressing the human element, which is the basic building block of society, in the context of social, psychological, medical, and educational. Especially social security, retirement system, increasing the quality of life of individuals in working life and social adaptation depend on the active contributions of social work. The network has played an important role in digitalization through IoT, digital and virtual applications [23]. Digitalization has serious risks as well as making life easier, social and financial support, education, and science [24]. Therefore, it is necessary to raise awareness in the context of network security and privacy in social work.

The elderly, children, women, disabled people, and people in need should be protected from the risky and negative effects of the network. Likewise, social work institutions should benefit from this protection. For this reason, it is important that social work beneficiaries and institution personnel receive training in order to create awareness.

Conclusion and Recommendations

Digital security is necessary for social work to ensure equality in society, to meet support needs, and to achieve environmental and social harmony. Cyber-attacks and potential system vulnerabilities can result in the disclosure of confidential information of the beneficiaries and the organization/institution. This leads to the disclosure of important information and serious damage. For this reason, private and public institutions where social work is carried out should take necessary measures for network security and privacy.

Actions can be taken by establishing risk groups and definitions. While creating risk groups, the beneficiaries and the risk groups belonging to the institution should be evaluated in different groups. Risk situations/levels within the groups should be determined according to the information monitored by spyware regarding the attempt to infiltrate the network. User names and passwords, corporate data, personal information of users, bank account numbers, social security numbers are among the information targeted by spyware.

Information and risk levels that pose a risk in every social work institution may create a difference. While the personal information of the elderly in nursing homes is risky, account numbers in social security institutions carry an element of risk. The risk factor is in the communication channels of the devices through spam in home care services. In particular, gerontological devices connected to Bluetooth, wireless connection devices, smart home systems, security alarms are among risky devices. Women's and children's shelters are intended to protect against external threats. Therefore, personal information and address create a high-risk level.

In social work, network security and privacy are important factors that should be taken into consideration personally and institutionally. While creating corporate strategy in social work, network users, risk factors, storing, and backing up information should be done successfully. Besides, necessary information security should be provided in inter-institutional relations and information exchange. It is important for each institution to create a strategy in determining the risk level and elements and to integrate it with the corporate strategy.

Empirical studies on the network security and privacy of social work institutions are recommended for future studies. Studies to be performed taking into account the international application differences will contribute to the social work field. Besides, social work beneficiaries should be interviewed and potential risk factors and negative experiences on this issue should be investigated.

References

1. Grinnell Jr, R M, Unrau Y (2005). Social work research and evaluation: Quantitative and qualitative approaches. Cengage Learning.
2. Wu A M, Tang C S, Yan E C (2005) Post-retirement voluntary work and psychological functioning among older Chinese in Hong Kong. Journal of Cross-Cultural Gerontology 20: 27-45.
3. Reisch M, Jani J S (2012) The new politics of social work practice: Understanding context to promote change. The British Journal of Social Work 42: 1132-1150.
4. Gray M, Webb S A (2013) The new politics of social work. Macmillan International Higher Education.
5. Ferguson H (2001) Social work, individualization and life politics. British Journal of Social Work 31: 41-55
6. Dababnah S, Parish S L, Brown L T, Hooper S R (2011) Early screening for autism spectrum disorders: A primer for social work practice. Children and Youth Services Review 33: 265-273.
7. Geiger D L (1978) Note: How future professionals view the elderly: A comparative analysis of social work, law, and medical students' perceptions. The Gerontologist 18: 591-594.
8. Gruber J, Wise D A (2009) Social security programs and retirement around the world: Fiscal implications of reform. University of Chicago Press.
9. Lambert E G, Pasupuleti S, Cluse-Tolar T, Jennings M, Baker D et al. (2006) The impact of work-family conflict on social work and human service worker job satisfaction and organizational commitment: An exploratory study. Administration in Social Work 30: 55-74.
10. Blaschke C M, Freddolino P P, Mullen E E (2009) Ageing and technology: A review of the research literature. British Journal of Social Work 39: 641-656.
11. Dickson D J, Dickson D T (1998). Confidentiality and privacy in social work: A guide to the law for practitioners and students. Simon and Schuster.
12. Chen M, Qian Y, Mao S, Tang W, Yang X et al. (2016) Software-defined mobile networks security. Mobile Networks and Applications 21: 729-743.
13. Evans M, McComb P (1999) Policy transfer networks and collaborative government: the case of social security fraud. Public Policy and Administration 14: 30-48.
14. Button M, Tapley J, Lewis C (2013) The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. Criminology & Criminal Justice 13 :37-61.
15. Gunawan B, Ratmono B M (2020) Social Media, Cyberhoaxes and National Security: Threats and Protection in Indonesian Cyberspace. IJ Network Security 22: 93-101.
16. Zhang Q, Xu D (2020) Security authentication technology based on dynamic Bayesian network in Internet of Things. Journal of Ambient Intelligence and Humanized Computing 11: 573-580.
17. Nife F N, Kotulski Z (2020) Application-Aware Firewall Mechanism for Software Defined Networks. Journal of Network and Systems Management 1-22.
18. Dias K L, Pongelupe M A, Caminhas W M, de Errico L

(2019) An innovative approach for real-time network traffic classification. Computer Networks 158: 143-157.

19. Wang S, Chen Z, Yan Q, Yang B, Peng L, Jia Z et al. (2019) A mobile malware detection method using behavior features in network traffic. Journal of Network and Computer Applications 133: 15-25.
20. Jardine E (2020) The Case against Commercial Antivirus Software: Risk Homeostasis and Information Problems in Cybersecurity. Risk Analysis 40: 1571-1588.
21. Bai L, Rao Y, Lu S, Liu X, Hu Y et al. (2019) The Software Gene-Based Test Set Automatic Generation Framework for Antivirus Software. JSW 14: 449-456.
22. Feng B, Li Q, Ji Y, Guo D, Meng X (2019) Stopping the cyberattack in the early stage: assessing the security risks of social network users. Security and Communication Networks 2019.
23. Mazzei D, Baldi G, Fantoni G, Montelisciani G, Pitasi A, Ricci L, Rizzello L et al. (2020) A Blockchain Tokenizer for Industrial IOT trustless applications. Future Generation Computer Systems 105: 432-445.
24. Cagle M N (2020) Reflections of Digitalization on Accounting:The Effects of Industry 4.0 on Financial Statements and Financial Ratios.In Digital Business Strategies in Blockchain Ecosystems 473-501.