Proceedings of the

18th European Conference on Digital Government
ECDG 2018

Hosted By
University of Santiago de Compostela
Spain

25 - 26 October 2018

Edited by
Prof. Dr. Ramon Bouzas-Lorenzo
and
Prof. Dr. Andres Cernadas Ramos

Copyright The Authors, 2018. All Rights Reserved.

No reproduction, copy or transmission may be made without written permission from the individual authors.

Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:
http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX http://tinyurl.com/ECDG2018 Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.
The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-912764-04-4
E-Book ISSN: 2049-1034
Book version ISBN: 978-1-912764-03-7
Book Version ISSN: 2049-1026

Published by Academic Conferences and Publishing International Limited
Reading
UK
44-118-972-4148
www.academic-conferences.org

Contents

MCDM Model for Evaluation of Social Network Security Threats

Rasim Alguliyev, Ramiz Aliguliyev and Farhad Yusifov
Institute of Information Technology of ANAS, Baku, Azerbaijan
r.alguliev@gmail.com
r.aliguliyev@gmail.com
farhadyusifov@gmail.com

Abstract: The popularity of social networks creates a high risk for the users. A large amount of personal data that users share on social networks makes them a target for a malicious person. A malicious person can obtain sensitive personal data simply by using social networks and can carry out many kinds of attacks, such as spam, malware, worms, sensitive data theft and so on. In this paper, the risks and security issues of social networks are explored. Various security and privacy threats targeted at each user of social networks are classified. Evaluation of social network security threats based on multi-criteria evaluation method is reviewed. This paper also proposes a fuzzy TOPSIS model for the evaluation of security threats. Social networks security threats are evaluated and ranked based on criteria such as interception of confidential information, reputation loss in government-citizen (G2C) relations and organization of social-political conflicts. In the numerical study, the social network security threats are evaluated and ranked according to selected criteria.

Keywords: social network, malicious user, security threat, fishing, multi-criteria evaluation, fuzzy TOPSIS

1. Introduction

Recently, the public administration is transformed into open governance format and government-citizen relationships are changed due to rapid development of ICT and the widespread use of social networks the (Karakiza, 2014; Dwivedi, et al., 2017; Alguliyev, & Yusifov, 2018). Specifically, social networks become one of a bilateral communication tool connecting government and society increasing government transparency and the growth of a democratic society (Banday, & Mattoo, 2013; Song, & Lee, 2016; Bergquist, et al., 2017). Transparency in governance can be reached through launching a feedback mechanism on government-citizen (G2C) relationships.

At present, social networks become very prevalent throughout the world. Millions of people are benefiting from various kinds of social networks that enable them to communicate with friends, relatives, and share personal data. Nevertheless, attractiveness of social networks also causes a great threat for their users (Novak & Li, 2012, Fire, Goldschmidt & Elovici, 2014; Rathore et al 2017, Kayes & Iamnitchi, 2017). Increasing volume of personal information shared by social network users turns them into an anticipated objective of the malicious users. Numerous privacy and security problems related to user data may occur when uploading multimedia content such as user photos, videos and so forth (Gao, et al., 2011; Dreßing, & et al., 2014; Fire, Goldschmidt, & Elovici, 2014; Kayes, Iamnitchi, 2017). Uploaded multimedia content may contain data shared through the virus which starts to be spread on the social network site and beyond its boundaries almost right after being uploaded. Malicious attacks may include seizure of sensitive personal data, including spam, malware, social bots, and data theft (Fire, Goldschmidt, & Elovici, 2014; Zhang, & Gupta, 2016; Rathore & et al. 2017). Moreover, the personal data seized for malicious purposes may be subject to serious cybercrime such as bank fraud or transaction fraud with the use of user-sensitive information (Zhang, & Gupta, 2016; Rathore et al 2017). many researchers believe that the attacks on social networks have a wide range of applications ranging from the personal data interception to malware distribution (Raggo, 2016; Rathore et al., 2017).

Several researchers and companies dealing with security issues offer different solutions to reduce potential threats concerning the growing social network threats (Cao, et al., 2016; Rathore & et al, 2017). Numerous studies focus on security issues in social networks (Novak & Li, 2012; Jin, & et al., 2013; Fire, Goldschmidt & Elovici, 2014; Zhang, & Gupta, 2016; Rathore & et al, 2017).

In this paper, social networks threats are analysed, and various current threats are reviewed. The goal of this study is to assess the potential threats in order to achieve a secure social networking ecosystem. Identifying, evaluating and preventing security threats to the social networks ensure understanding the basic principles and perspectives of the security concept of social networks. Furthermore, potential threats to social security are evaluated and the perspective research trends are specified.

2. The risks and security issues of social networks

Social networks have a significant impact on the performance of governments. For example, as a result of the survey, it has been shown that the impact of social media on the political activity of citizens is increasingly important (Grubmüller, Götsch, & Krieger, 2013; Park, et al., 2016). Experts note that social media will help governments to become more transparent by providing citizens with better service and access to information, by opening an active channel with them, and ultimately empowering citizens (Khasawneh, & Abu-Shanab, 2013; Song, & Lee, 2016). Also, if governments effectively use such sites, it will enable them to become more effective and active participants in society. In terms of e-participation, social media provides new communication tools to quickly and efficiently deliver any message or news from governments (Aladalah, Cheung, & Lee, 2015; Alguliyev, & Yusifov, 2018). Citizens can participate in online discussions with their local and national governments on issues of public interest. This will create a more open, transparent and mutually acceptable relationship between citizens and governments (Alguliyev, & Yusifov, 2018).

It should be noted that public authorities using social networking analyses pay attention to people as citizens and not as customers and consumers, and expand their activities in public-political areas. Therefore, social media analytics aimed at government purposes require better judgment for the legal and ethical aspects of various reasons (Grubmüller, Götsch, & Krieger, 2013; Park, et al., 2016).

First, the concept of confidentiality in social media is almost completely changed (Rathore et al., 2017). Participants are less concerned to share personal information about themselves and their friends. It is extremely difficult for the user to distinguish what information is for public or private use. The concept of confidentiality is becoming increasingly incomprehensible and in general, the lack of clear media confidentiality in ICT field and social media accelerates this process. While the problem of confidentiality seems to be less important for social media users, empirical evidence suggests that such concerns are rising when users communicate directly with government agencies (Silic, & Back, 2016, Rathore et al 2017, Facebook[1,2], 2018). As a result, citizens' acceptance of the use of the social media by the governments requires legitimacy. Therefore, it is essential for governments to comply with the existing legal norms to ensure the safety and confidentiality of citizens' information (Park, et al., 2016).

To protect confidentiality, governments should only use publicly available information. This means that with the help of appropriate analytical tools should collect citizens' information they share in their personal accounts, but they must limit them to public listed posts.

Social networks provide extensive opportunities for hackers to identity theft. In such types of attacks, a malicious person, without the user's consent, can intercept his or her personal information, including bank accounts, phone numbers, addresses etc., and use them to commit cybercrime. For example, many social networks, such as Facebook, offer game apps to their users. These applications require personal information such as user credit card information, phone number, email address etc. to complete the registration process. Of course, the risk of personal data theft and phishing attacks is increased when a user provides the phone number and credit card information. In some cases, applications may cause the user to resort distract the user’s attention to harmful content and damage their reputation.

One of the most noticeable potentially harmless options in the social networking context can be the unauthorized use of personal information for advertisement purposes, selection of the potential the acquaintances or selection of content that may be of interest. The transfer of personal data from various social networks has already been confirmed for a fact (Facebook[1,2], 2018; Rathore et al 2017). One of the biggest problems for users is that, as a consequence of the social network's fault, multiple user-specific data leakage may be noted within the framework of various projects. One of the causes of serious disturbance is the hacking of user accounts or account loss and the intercept of all personal information. When this situation becomes massive, more serious problems occur. There are many potential threat to users such as technical vulnerabilities, viruses, trojan horse, phishing and other malicious software and can be used to intercept the user's confidential information (Raggo, M. 2016, Silic, & Back, 2016). Phishing attack is one of the most widespread attacks by cybercriminals in the opinion of experts, and the main target is Internet payments, Internet banking, online games, Internet stocks, Web 2.0 technology used sites and so on (Silic, & Back, 2016; Rathore et al 2017).

Another important issue is that many companies collect information from different sources, third-party resources, including social networks to create a user profile to sell products and disclosure user behaviour. Social network users are unable to determine for which purpose the shared data will be used, due the unauthorized collection of user's data and the unawareness of the users about these technologies. For example, user data can be transmitted to law enforcement for security reasons or may be used by the vendor for marketing purposes. In this regard, social networking profile, collected large volume of personal data, the user behavior data etc. can directly affect the user (CareerBuilder; Facebook[1,2], 2018; Khan, Swar, & Lee, 2014; Silic, & Back, 2016; Rathore et al 2017).

In literature, threats are classified into 4 categories (multimedia content threats, traditional threats targeting personal information, social-oriented threats, threats to children safety) (Fire, Goldschmidt, & Elovici, 2014; Kayes & Iamnitchi, 2017). Social network threats can be categorized as shown in Table 1.

The first category includes multimedia content threats used to user profiles disclosure. Obviously, content sharing is one of the most important functions of social networks. The most common form of this type of data is multimedia content. However, shared high-quality images, videos are used in a variety of ways, increasing the probability of interception of location information, face recognition, and other data and creates conditions for illegal use.

Table 2: Social networks security threats

Content oriented threats	**Traditional threats targeting personal information**	**Social threats and threats targeting children**
Multimedia content exposure	Phishing	Corporate espionage
Disclosure of sensitive information	Malware	Cyber-stalking / Cyber-blackmail
Content manipulation	Fake profiles	Cyber-grooming / Cyber-bullying
Metadata disclosure	Spam	Reputation loss
Links disclosure and redirection	Fake links	Encouraging social confrontation on racial, ethnic and religious grounds
Unauthorized access to videoconferences / messages	Violation of user anonymity	Destructive provocation
Fake tagging and sharing	Profile cloning	Cyber-suicide / Internet addiction
Unauthorized disclosure and use of information	Disclosure of relations	Creating target groups

The second category includes traditional threats. Vulnerabilities in the social network infrastructure are used to attack users in different ways. Phishing, malicious software for intercepting personal data etc. can be shown as traditional attack methods. This information is used as a very effective tool for malicious acts. Malicious person can commit more serious cybercrimes after intercepting confidential information, bank information etc.

The third category includes social threats. These threats have more coverage and disclosure of social relationships among social network users is a potential threat to them. Malicious persons may deliberately commit cyber-crime against a certain social group, for example a company employee, by disclosing the relationships between social network users in different ways. For example, people from different social groups can be instigated to commit cybercrime, espionage, share malicious information etc., being motivated by offered gifts, money or due to blackmail.

The fourth category includes threats targeting children and teenagers. Obviously, children and teenagers face many threats on social networks. However, there are a number of threats that specifically target young people and teenagers in the social network. These threats include children's cyber-bullying, cyber-stalking, cyber-blackmail, cyber-grooming, abuse of trust, and so on. For example, in some cases cyber threats to children can have disastrous consequences, and in practice, there are facts about children committing suicides to end their lives (Fire, Goldschmidt, & Elovici, 2014).

3. Multi-criteria evaluation model for evaluation social networks threats

In literature, Multi-criteria decision making model (MCDM) methods can be used in various fields, such as personnel selection, selection of equipment in production, projects selection, etc. Literature analysis shows that multi-criteria evaluation methods have been applied in various fields such as personnel selection, projects

assessment, candidates ranking, equipment assessment, and so on. (Khorami & Ehsani, 2015; Tuan, 2017; Afshari et al 2017). Over time, MCDM models have found its application in solution of various complex issues of decision-making. AHP, TOPSIS, VIKOR, PROMETHEE, ELECTRE, SAW, MOORA, MULTIMOORA and other methods were used to solve decision-making problems (Karabasevica, 2015; Alguliev et al 2016; Khorami & Ehsani, 2015; Mardani et al 2015, Khorami & Ehsani, 2015). There are research studies on the comparison and review of MCDM methods (Turskis & Zavadskas, 2011; Stanujkic et al., 2013; Zavadskas et al., 2014; Mardani et al 2015, Khorami & Ehsani, 2015). Literature analysis shows that there are numerous research studies on the application of fuzzy MCDM methods. Fuzzy MCDM are widely used to rank the soltuion alternatives characterized by fuzzy values based on multiple criteria (Kelemenis & Askounis, 2010; Rouyendegh & Erkan, 2013; Alguliyev, et al, 2016, Tuan 2017).

A model for evaluating the social networks security threats based on the fuzzy TOPSIS (Technique for Order Preferences by the Similarity to Ideal Solution) method is proposed in this paper. The TOPSIS method allows calculating an integral index for alternatives taking into account many criteria and provides ranking of alternatives for the procedure of selection the options with the decision maker. The Fuzzy TOPSIS method was used to select and rank the alternatives and make group decisions in a number of application issues (Capaldo, & Zollo, 2001, Dursun, & Karsak, 2010; Kelemenis, & Askounis, 2010; Chang, Yeh, & Chang, 2013; Rouyendegh & Erkan, 2013; Alguliyev, et al., 2016; Tuan, 2017). Let's note that the most commonly used AHP (Analytical Hierarchy Processes) method for multi-criteria ranking of alternatives has a number of deficiencies. This includes difficulty of calculation, contradiction of expert estimates due to large number of experts etc. (Alguliyev, et al., 2016).

Let's review the evaluation of social network security threats based on fuzzy TOPSIS method.

Let's say that n as a number of alternative sets A_i, $i = 1,2,...,n$ must be evaluated by a group of K decision makers E_k ($k = 1,2,...,K$) based on m number of criteria C_j, $j = 1,2,...,m$. In proposed approach the criteria are not inter-dependent, are equally important and can be evaluated.

Evaluation is carried out by each decision maker E_k in order to determine decision matrix $S^k = \left\| s_{ij}^k \right\|, i = 1,2,...,n$; $j = 1,2,...,m$; $k = 1,2,...,K$.

TOPSIS method consists of following stages (Chang, Yeh, & Chang, 2013; Alguliyev, et al. 2016)**:**

- Step 1. Creating a decision matrix.
- Step 2. Choose of linguistic variables for the alternatives with the respect to criteria.
- Step 3. Calculation of aggregate fuzzy rating for alternatives.
- Step 4: Normalize the aggregate fuzzy decision matrix.
- Step 5: Creating normalized fuzzy decision matrix.
- Step 6: Determine of fuzzy positive ideal solution and fuzzy negative ideal solution.
- Step 7: Calculate the distance of each alternative from the fuzzy positive ideal solution and fuzzy negative ideal solution.
- Step 8: Calculation of closeness index of each alternative.
- Step 9: Ranking the alternatives.

4. The formulation experimental study

Let's assume that malicious attacks are committed against social network users. Social network security threats are likely to be: A_1 - phishing; A_2 - fake user profiles; A_3 - unauthorized access to user messages; A_4 - sensitive information disclosure; A_5 - cyber-stalking. The criteria used to evaluate the threats include: C_1 - interception of confidential information; C_2 - reputation loss in government-citizen (G2C) relations; C_3 - organize of social-political conflicts.

Let's assume that in this case, five alternative (security threats) sets A_i ($i = 1,2,...,5$) are evaluated by a group consisting of five decision makers (experts) E_k, in relation to three criteria C_j ($j = 1,2,...,m$).

The appropriate linguistic variables are represented to evaluate alternatives to each criterion. Decision makers use the TFN linguistic variables provided in Table 1 to evaluate alternatives in relation to criteria.

Table 1: Linguistic variables for threat evaluation

Linguistic variables	TFNs
Very high	(8,9,10)
High	(6,7,8)
Medium	(4,5,6)
Weak	(2,3,4)
Very weak	(1,1,2)

Let's assume that according to steps 1-4, the normalized aggregate fuzzy decision matrix for benefit criterion is shown in Table 2**.**

Table 2: Normalized aggregate fuzzy decision matrix

Alternatives	Criteria		
	C_1	C_2	C_3
A_1	(0.636,0.750,0.864)	(0.333,0.417,0.556)	(0.412,0.500,0.647)
A_2	(0.455,0.568,0.682)	(0.639,0.750,0.889)	(0.588,0.735,0.882)
A_3	(0.773,0.886,1.000)	(0.722,0.861,1.000)	(0.353,0.441,0.588)
A_4	(0.205,0.250,0.364)	(0.583,0.694,0.833)	(0.559,0.676,0.824)
A_5	(0.455,0.568,0.682)	(0,417,0.528,0.667)	(0.735,0.853,1.000)

Table 3: Security threats ranking

Security threats	CI_i	Rank
A_1	0,421	**4**
A_2	0,546	**2**
A_3	0,573	**1**
A_4	0,389	**5**
A_5	0,521	**3**

As described in Table 3, according to Steps 8 and 9, A_i alternatives are ranked by descending order based on CI_i closeness index values. Social networks security threats are ranked in accordance with A_3, A_2, A_5, A_1 and A_4 sequence and the criteria of unauthorized access to user messages is the greatest threat to the social network security.

5. Conclusion

Social networks are very popular among users and the number of users is growing rapidly. Nevertheless, the popularity of social networks creates potential threats to their users. Rapid increase in the volume of personal data shared by social network users turns them into a desirable target of the malicious people. Currently, various attacks are carried out against social networks and these are considered a major threat to users. In this paper, potential security threats to social networks were analyzed and classified. The attacks on social networks were classified into 4 categories (multimedia content threats, personal information security threats, socially directed threats, threats targeting children). The paper offered a multi-criteria evaluation method to analyze social security threats. Potential threats are categorized in relation to the criteria determined by the fuzzy TOPSIS

method. Based on the proposed approach, the threats were evaluated and ranked based on criteria such as interception of private data, reputation loss in government-citizen (G2C) relations and organization of social-political conflicts. In future studies, empirical research will be preferred using hybrid methods to evaluate threats in order to form a safe and secure social network eco-environment.

Acknowledgements

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan - Grant № EİF-KETPL-2-2015-1(25)-56/05/1

References

Afshari, A.R., Nikolić, M., Akbari, Z. (2017), Personnel selection using group fuzzy AHP and SAW methods, Journal of engineering management and competitiveness, 7(1), 3-10

Aladalah M., Cheung Y. & Lee V. (2015) Enabling Citizen Participation in Gov 2.0: An Empowerment Perspective. Electronic Journal of e-Government, 13(2).

Alguliyev R.M., Aliguliyev R.M., Mahmudova R.M. (2016). A Fuzzy TOPSIS+Worst-Case Model for Personnel Evaluation Using Information Culture Criteria. *International Journal of Operations Research and Information Systems*, 7(4), 38-66.

Alguliyev, R.M. & Yusifov, F.F. (2018) The Role and Impact of Social Media in E-Government, Book Chapter in Alcaide-Muñoz L. & Alcaraz-Quiles F. J. (Eds.) *Optimizing E-Participation Initiatives Through Social Media (pp. 28-53)*, The Advances in Wireless Technologies and Telecommunication book series, USA, IGI Global.

Banday, M.T., & Mattoo, M.M. (2013). Social Media in e-Governance. *Scientific Research Journal*, 47-56.

Bergquist, M. & et al., (2017). From e-government to e-governance: social media and public authorities legitimacy work, In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarres, Portugal, June 5-10, 858-872.

Cao, J. Li, Q. Ji, Y. & et al., (2016). Detection of forwarding-based malicious urls in online social networks, Int. J. Parallel Program, 44 (1), 163–180.

Capaldo, G., Zollo, G. (2001). Applying fuzzy logic to personnel assessment: A case study, *Omega*, 29(6), 585-597

CareerBuilder, Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade, www.careerbuilder.com, Online accessed 15 April 2018.

Chang, Y.-H., Yeh, C.-H., & Chang, Y.-W. (2013). A new method selection approach for fuzzy group multicriteria decision making. Applied Soft Computing, 13(4), 2179–2187. doi:10.1016/j.asoc.2012.12.009

Dreßing, H, Bailer, J., Anders, A. et al. (2014), Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims, Cyberpsychol, Behav. Soc. Netw. 17 (2) 61–67.

Dursun, M. & Karsak, E.E. (2010). A fuzzy MCDM approach for personnel selection. *Expert Systems with Applications*, 37, 4324-4330.

Dwivedi, Y.K., & et al. (2017) Exploring the Role of Social Media in e-Government: an Analysis of Emerging Literature. ICEGOV 2017, 97-106.

Facebook[1] suspends 200 apps over data misuse investigation, 2018, https://www.reuters.com, Online accessed 15 April 2018.

Facebook[2] temporarily blocks new apps from joining its platform, 2018, www.theverge.com, Online accessed 15 April 2018.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions, IEEE Commun. Surv. Tut. 16.(4), 2019-2036.

Grubmüller, V., Götsch, K., & Krieger, B. (2013). Social media analytics for future oriented policy making, European Journal Futures Research, 1:20.

Jin, L., Chen, Y. Wang, T. & et al. (2013). Understanding user behavior in online social networks: a survey, IEEE Commun. Mag. 51(9), 144–150.

Karabasevica, D., Stanujkic, D., & Urosevic, S. (2015) The MCDM model for personnel selection based on SWARA and ARAS methods, *Management*, 77, 43-52

Karakiza, M. (2014). The impact of Social Media in the Public Sector. *Proceedings of the International Conference on Strategic Innovative Marketing*, 384-392.

Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey, Online Social Networks and Media, 3–4, 1–21.

Kelemenis, A., & Askounis, D. (2010). A new TOPSIS-based multi-criteria approach to personnel selection, Expert Systems with Applications, 37, 4999–5008.

Khan, G.F., Swar, B., & Lee, S.K. (2014) Social Media Risks and Benefits: A Public Sector Perspective, Social Science Computer Review, 32(5), 606-627.

Khasawneh, R. T., & Abu-Shanab, E. A. (2013). E-Government and Social Media Sites: The Role and Impact. *World Journal of Computer Application and Technology*, *1*(1), 10–17.

Khorami, M., & Ehsani, R. (2015). Application of Multi Criteria Decision Making approaches for personnel selection problem: A survey, International journal of engineering research and applications, 5(5), 14-29.

Mardani, A., Jusoh, A., & et al. (2015). Multiple criteria decision-making techniques and their applications – a review of the literature from 2000 to 2014. Economic Research – Ekonomska Istrazivanja, 28(1), 516-571.

Novak, E., Li, Q. (2012) A Survey of Security and Privacy in Online Social Networks, College of William and Mary Computer Science, Technical Report, 1–32.

Park, M.J., Kang, D., Rho, J.J., & Lee, D.H. (2016). Policy Role of Social Media in Developing Public Trust: Twitter communication with government leaders. *Public Management Review*, *18*(9), 1265–1288. doi:10.1080/14719037.2015.1066418

Raggo, M. (2016) Anatomy of a Social Media Attack, www.darkreading.com/analytics/anatomy-of-a-social-media-attack/a/d-id/1326680. Online accessed 14 May 2018.

Rathore, Sh., Sharma, P.K., Loia, V. & et al. (2017). Social network security: Issues, challenges, threats, and solutions, Information Sciences, 421, 43–69.

Rouyendegh, B.D., Erkan, T.E. (2013). An application of the fuzzy ELECTRE method for academic staff selection, *Human Factors and Ergonomics in Manufacturing and Service Industries*, 23(2), 107-115.

Silic, M. Back, A. (2016) The dark side of social networking sites: Understanding phishing risks, Computers in Human Behavior, 60, 35-43, http://dx.doi.org/10.1016/j.chb.2016.02.050.

Song, C., & Lee, J. (2016). Citizens' Use of Social Media in Government, Perceived Transparency, and Trust in Government. *Public Performance & Management Review*, *39*(2), 430–453. doi:10.1080/15309576.2015.1108798

Stanujkic, D., Djordjevic, B., Djordjevic, M. (2013). Comparative analysis of some prominent MCDM methods: A case of ranking Serbian banks. Serbian journal of management, 8(2), 213-241.

Tuan, N.A. (2017). Personnel Evaluation and Selection using a Generalized Fuzzy Multi-Criteria Decision Making. *International Journal of Soft Computing*, 12 (4), 263-269.

Turskis, Z., & Zavadskas, E. K. (2011). Multiple criteria decision making (MCDM) methods in economics: an overview. Technological and economic development of economy, (2), 397-427.

Zavadskas, E. K., Turskis, Z., & Kildienė, S. (2014). State of art surveys of overviews on MCDM/MADM methods. Technological and Economic Development of Economy, 20(1), 165-179.

Zhang, Z., & Gupta, B.B. (2016) Social media security and trustworthiness: Overview and new Direction, Future Generation Computer Systems, Elsevier, https://doi.org/10.1016/j.future.2016.10.007