PREGLEDNI RAD – REVIEW SCIENTIFIC ARTICLE 10.7251/ZRPIM2201441J

INFORMATION SECURITY AS A SEGMENT OF SOCIAL NETWORK ACCOUNT AUDIT

Nemanja I. Jakovljević

University of Belgrade, Faculty of Economics, Kamenička Street 6, 11000 Belgrade, Serbia,
jakovljevic.i.nemanja@gmail.com

ABSTRACT

Information security includes a list of measures whose appropriate application ensures that the data contained in information systems are sufficiently protected from unauthorised access, unauthorised changes and unauthorised use, ensuring the integrity, confidentiality and availability of data in information systems. Information security is an essential and unavoidable aspect of any audit of accounts on social networks, which is carried out in natural conditions by applying methodological guidelines on a specific statement on a particular social network. A social network account audit is an independent review of an external person on the status of social media accounts, account activities and accounts information security. Nowadays, social networks are an essential factor in many people's daily lives, which suggests that they contain a large amount of information about users that can be confidential and sensitive and include photos, videos, payment card information, location, activities, and more. Thus, the security of social network users is, directly and indirectly, related to the security mechanisms of logging in to the network and how social network managers manage user data. The subject of research in this paper is the theoretical presentation of the importance of information security in the context of social network account audit by describing the challenges, risks and recommendations that conduct tests and draw conclusions about information security accounts on social networks. The main finding in the paper is that persons engaged in the social network account audit in each audit engagement should pay special attention to the information security of demands as an essential segment of the audit of rankings on social networks.

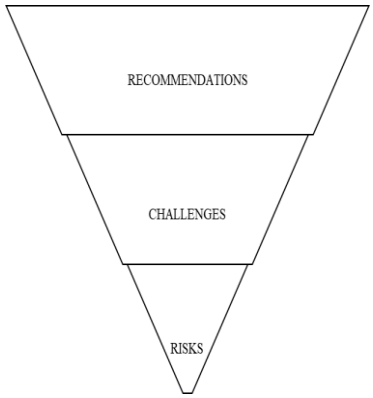
Keywords: information security, auditors, social network account audit, social networks.

INTRODUCTION

Information security includes a list of measures whose appropriate application ensures that the data contained in information systems are sufficiently protected from unauthorised access, unauthorised changes and unauthorised use, ensuring the integrity, confidentiality and availability of data in information systems. Information security is an essential and unavoidable aspect of any social network account audit, which is carried out in natural conditions by applying methodological guidelines on a specific account on a particular social network. A social network account audit is an independent review of an external person on the status of accounts on social networks, account activities and information security of the account. Nowadays, social networks are an essential factor in the daily lives of a large number of people, which suggests that they contain a large amount of information about users that can be confidential and sensitive and include photos, videos, payment card information, location, activities and more. . Thus, the security of social network users is, directly and indirectly, related to the security mechanisms of logging in to the network, as well as how social network managers manage user data.

Social network account audit is one of the modern concepts in social media management. A social network account audit is an independent review (Jakovljević, 2021a) and analysis of social media accounts of the entity (Quesenberry, 2015) or persons, including an overview of social media activities, media publishing and advertising goals, compliance goals, security status determination and other. The general objective of social network account audit, in addition to providing independent assurance, may include providing an overview of tool, techniques and

competencies available to the entity or person to identify weaknesses, improve performance, and improve social media positions. A social network account audit is a comprehensive, systematic analysis of the environment in the form of social networks of the subject entity, both internal and external. It includes the organisation's goals (Gattiker, 2014), strategies and principles to identify problems or areas of opportunity (Jakovljević, 2021b) and recommend the course of action (Jakovljević, 2021c) that best suits the business needs of the entity or person (Jakovljević, & Jakovljević, 2021). At first glance, there are no points of contact with traditional audits, such as financial statements audits or regularity audits. In principle, it has no essential equality with audit as an independent assurance service (Jakovljević et al., 2021). However, it can have it if it is carried out by an external person with expertise in the field of social media management and if it is engaged in providing independent and objective assurance of the status of a particular account in a specific social network, its security and, consequently, the protection of the account holder. A significant number of people have accounts with many followers who interact with the account holder daily by expressing reactions to his announcements. Such accounts are an essential funding source for individuals or a significant business segment for particular companies based on social networks.



Graph 1. Three segments of information security through social network account audit.

Social networks provide an effective way to connect between people and share personal content such as photos, texts, videos and more. However, the lack of attention and caution when sharing unique content can lead to serious unintended consequences, whether personal or business orders. Unauthorised persons and attackers can often use social media accounts as a simple mechanism to achieve their goals, including misrepresenting and distributing suspicious links and questionable content by interacting with other accounts that become victims of fraud by opening received content. Therefore, a greater degree of attention when performing activities on social networks is desirable. In cases of professional account management, there is a need to examine the information security of orders on social networks through the revision of demands on social networks. There are many cases in which companies or celebrities who had accounts on social networks with many followers found themselves denied access to the account and permanent loss, which can pose a serious challenge to business and reputation. The methods used by attackers depend on the target social media platform. For example, Facebook allows users to transfer published photos and comments to privacy status, so the attacker will often be friends with the target user's friends or send a friend request to the target user directly to access their posts. If an attacker can connect with several friends of the target user, then the target user is more likely to accept a friend request based on the number of connected friends. LinkedIn is another common target because it is known for business networking, and user networks are usually data on employees in the same organisation. LinkedIn is a convenient social network for collecting business addresses for phishing attacks if an attacker targets a business account. A large business entity may have several networked employees list their employer and titles.

An attacker can use this public information to find several employees who have access to financial information, private customer data, or access to a network with high authority. False brand representation is another challenge in the domain of social media accounts. With enough information gathered, an attacker can impersonate a business brand to trick users into sending money, revealing private information, or providing attackers with account access parameters. Attackers also use this threat to attack scripting in multiple locations or falsify requests in numerous places. These attacks can lead to massive data leaks and business infrastructure threats. Gathering information for data theft is not the only reason attackers use social network accounts. Information published on social networks can obtain passwords or misrepresent business users. Many accounts allow users to reset passwords if they enter a security question. With enough data from social media posts, an attacker could guess the answer to these security questions based on private information posted by the target user. The research subject in this paper is the theoretical presentation of the importance of information security in social network account audit by describing the challenges, risks and recommendations that conduct research and draw conclusions on information security of accounts on social networks.

RISKS

The number of users who have accounts and access social networks is increasing from year to year. The increase has been particularly pronounced in the last two years under the influence of the Covid 19 pandemic. Networks were observed both from the aspect of the account holder and from the part of persons engaged in the social network account audit. Probably the most present risk of all is identity theft. Many social media account providers publish a certain amount of their personal information to register on one or more social media platforms. This information becomes vulnerable because unauthorised persons and identity thieves use this information to reset passwords and apply for loans. Or other malicious purposes, such as opening another account with the same name and the same profile photo and other profile characteristics, in a way that makes it very difficult to determine which account is the right one (Nasirpouri, & Biros, 2021). For this purpose, copyright protection of a personal domain based on a specific account on a particular social network can be used. Another widespread scam is a type of intimate connection in which an unauthorised party, through the development of personal relationships and a sense of intimacy with the person accessing the account, creates an atmosphere of trust through which he achieves an unauthorised access account. A person who accesses a specific account on a particular social network in this way primarily uses some form of blackmail addressed to the owner of the account, which can be based on claiming a certain amount of money, publishing confidential data and more. This form of fraud is complicated to prevent. Still, it can be limited to reasonable limits by requiring, for example, two-factor authentication, which involves double authentication, or accessing devices from which the account is accessed will have open access in case planned activities are not performed. All activities performed on order in instances where the account management is professionalised and when an external person implements it should be designed, implemented according to a defined plan and completed at least some minimal form of supervision.

Contracting the management of orders on social networks should be a job that will be approached very carefully and with an appropriate dose of professional objectivity. The termination clause must be defined in such a way as to protect both contracting parties, especially the owner of the order, primarily in the domain of parameters for access to the order. When the contract is terminated, or the contract expires, the owner must have a specific notice period in which he will be able to change the parameters for accessing the account in such a way that the persons who managed the order after the contract termination will not be able to access the account. If the cancellation procedure is not adequately defined sufficiently, it can be a significant risk in the context of social media orders. Auditors may be inclined to review contracts entrusted with the management of social media accounts and, in cases where they find that this area is not adequately defined, may recommend explaining and signing an annexe to the contract that will sufficiently explain the subject matter. Dissatisfied employees working on social media account

management tasks can pose a risk. People can often react impulsively to events that may or may not be related to social media accounts and often show their resentment to their colleagues or bosses unexpectedly and without thinking. They can intentionally reveal sensitive data in their posts, which can significantly damage the reputation of a particular account in a specific social network.

Challenges

Information security in all its aspects is a significant dimension in the revision of orders on social networks and an unavoidable step during its implementation. In general, challenges are situations in which there is a threat to maintaining information security when doing business on social networks. In the context of social networks, challenges represent an increased degree of risk in activities in the field of account management on social networks, which may directly or indirectly impact the owner of the account on social networks. In cases where the direction of social media accounts is entrusted to a third party, there is a gap in expectations because conflicting interests may arise between the owner of a particular account in a specific social network and the person managing that account (Jakovljevic, 2021d). Therefore, the social media account manager is faced with a set of challenges that they must face to meet pre-defined goals and improve the management of social media accounts. At the same time, the same group of challenges is posed to independent, objective and professional persons engaged in the social network account audit and who need to perform an independent review of activities on a particular account in a specific social network.

As there has been a sudden expansion of social networks that have grown, covering an increasing number of user accounts, various benefits have caused severe problems in information security on social networks. The data privacy challenge requires preserving confidential and sensitive data on a specific account on a particular social network or is related to the account and can be accessed through the account. Communication that contains external links is mainly realised through the inbox of accounts on social networks and involves messages of different content, mostly funny or financially attractive, including a link that accesses the site with threatening content (Menard, Bott, & Crossler, 2017). It is recommended that messages from unknown and unverified accounts that contain external links that can be characterised as suspicious should not be opened. The challenge for information security in social network account audit in the field of malware includes testing the resistance of accounts to virus attacks. Malicious software in the form of viruses often finds its way to operating systems on devices that access accounts on social networks, most often through harmless advertisements and advertisements (Lin, Yang, Zhang, Xue, & Haga, 2021). The moment an unwanted party accesses the device's operating system, they are more likely to access social media accounts and steal confidential and sensitive data, or in some instances, to cause a complete collapse of the computer system.

In addition to the above challenges, legal challenges are associated with using social media accounts, such as posting offensive content against any individual, community or state. Offensive announcements, insults of vulnerable social groups and national minorities and discrimination may be subject to criminal provisions in terms of the legislation of a particular state, whose owner of a specific account in one particular social network is a citizen. Assessing possible financial outflows based on the payment of fines is an essential segment in the social network account audit. Today, most applications require permission from users to access personal information such as contacts, images, and current geographical location before installation. Some of these applications running in the background can download a virus on a user's phone or smartphone without his knowledge (Jingguo, Zhe, Gupta, & Rao, 2019). Every activity on the Internet leaves a trace, i.e. a path, data and information. When someone creates a new account on social media and provides details such as date of birth, name, location, personal habits and without our knowledge, all this information is used and shared with third parties for targeted advertising. This can cause security issues because third parties can collect real-time updates about the user's location.

Recommendations

Creating passwords with a strong composition is undoubtedly the primary option when defining parameters for enhanced security of social media accounts and ensuring the privacy of data and information stored on the account, whether a business account or a personalised account (Jassim, Al-Zahir, & Khazraji, 2022). Passwords should be complex and include different characters and different types of surfaces. This means that they should consist of letters and numbers and small and large characters, and of course, special characters in such an arrangement that implies a random choice of characters (Kajtazi et al., 2021). Such passwords provide a higher level of account security and deter unauthorised persons from accessing confidential and sensitive account information. Passwords should be remembered, and it is not recommended to write them down, whether on a computer, phone or paper. When logging in to an account, the auto-fill option can be pretty simple to quickly log in to an account on a social network. However, it stores the password either on the device or on the system and can be leaked and taken over by unauthorised persons. Also, with the auto-fill option, the password content and character order may be forgotten, which poses new challenges for account security on social networks, and again may depend on the cognitive abilities of the person accessing the account, age, attention and others. Persons who engage in social network account audits usually analyse and test the password's strength for access to the account during the audit engagement on a specific account. Suppose they find that it is weak or simple and easily detectable by unauthorised persons. In that case, they can recommend that the account holder establish a stronger password in accordance with generally accepted rules for creating strong passwords to increase the information security of the account itself on social networks (Kaušpadeiene, Ramanauskaite, & Čenys, 2019). Sharing content in posts, stories, and other forms of interaction is another challenge for social media accounts' information security and are emerging as an important social network account audit segment. Observed from information security in the social network account audit, it is inadmissible to publish personal data, such as date of birth, unique identification number, telephone number, data on family members, account number, etc. Such information must be permanently excluded when creating content for publication and must be considered strictly confidential and sensitive. In this context, it is possible to recommend that such content be removed from publications if they have already been published or draw the account holder's attention to the fact that account managers may not publish the above information. Suppose the rule on non-disclosure of this type of data was formalised, yet it was published. In that case, persons engaged in the social network account audit, have an obligation to conduct additional in-depth tests to determine how such situations have occurred. Persons who have published confidential content must be subjected to some form of sanction that may include fines, denial of access to the account or even, in extreme cases, and permanent cancellation of any form of business cooperation.

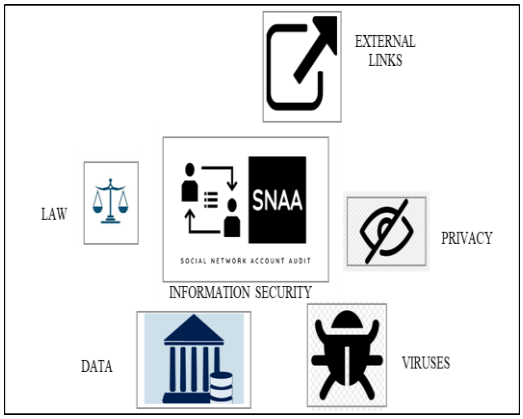
Persons who engage in social network account audit usually, during the audit engagement on a specific account, perform an analysis of the locations from which the order is accessed and the frequency of access to the demand from certain places and at certain times. Also, persons engaged in the social network account audit can examine and determine whether the account was accessed from private or shared networks during the time period that is the subject of the social network account audit. Access to the account from shared networks can be compassionate and high risk for the security of accounts on social networks. Therefore, those engaged in social media account audit may recommend that the owner of a particular account in a specific social network use private networks when accessing the account or use certain forms of protection, such as the privacy option when using shared networks. Persons engaged in the social network account audit during the implementation of control tests can record the procedure of access to the account and account management. In some instances, it is possible to determine the existence of so-called "open screens", whether they are computers, tablets or mobile phones (Ibnugraha, Nugroho, & Santosa, 2021). These are cases in which the person who accesses the account leaves it unlocked and edited with an open account after logging in to the account and performing certain activities.

This is the easiest way for unauthorised people to access the account. They can approach the device to misappropriate it or change the login parameters on the account, thus permanently

denying the account holder access to the account. Such cases represent severe failures in control mechanisms and can lead to the permanent loss of a specific account on a particular social network. Persons engaged in the social network account audit can therefore recommend to the account holder to improve control mechanisms and strengthen supervision over the activities on the account. Regularly updating the operating systems on the devices from which the account is accessed prevents the appearance of security holes, maintains the system at a high-security level with all the accompanying patches and prevents the spread of viruses through phishing, cracked software and more. Persons who audit (Jakovljevic, 2021e) accounts on social networks usually analyse the security status of the operating system during the audit engagement on a particular account. If they identify certain deficiencies, they can recommend the owner of a specific account in one particular social network to take action to update software. The overall information security of the account would be raised to a higher level. The lack of antivirus software can pose an additional challenge to the information security of social media accounts. Persons engaged in social network account audits may recommend that antivirus software be installed on the devices from which the account is accessed and that antivirus software is kept up to date to provide additional security for a specific account on a particular social network.

CONCLUSIONS

People worldwide use social networks to communicate, share personal photos, plan events, comment on current events and many other activities. Social networks have replaced traditional forms of communication and even some more modern ones, such as telephone calls or email. Fun games are played on social networks, and products are bought that leave personal and sensitive data such as account number, payment card data, an internet link to the wallet with cryptocurrencies, location, codes, close accounts and more (Chung, Xiaojun, James, & Zan, 2021). Therefore, it is essential that people who use social networks are aware of the risk on social networks, whether they are private or business activities or whether they use them for personal purposes or manage accounts for the benefit of others or social network account audit. One of the beneficial activities to increase the security of accounts on social networks can be to pay more attention to the management of logging in or logging into the account. Some social networks notify the account holder when the login is done from another location or another device. Some social networks even inform the account holder when the login attempt is unsuccessful. These are two excellent indicators that need to be monitored. In situations where they occur more often in short time intervals, a problem can be identified and solved in several ways. One of them can be the replacement of an existing password with a stronger password that will be composed of a combination of uppercase and lowercase characters, i.e. characters, letters and numbers in social networks that allow it.



Graph 2. Information security in social network account audit.

Sometimes changing the username or username can be helpful. Still, some social networks do not allow frequent changes of username, which means that care must be taken when choosing a new username and the existence of requirements to change the username. All other Internet sites where the account shortcut was listed included a changed username. Social networks are full of links to other external sites. By clicking on such links and visiting external locations, there is an increased risk of potentially infecting the account, often infecting the device from which the account was accessed when the link was opened. Therefore, people who use accounts on social networks can use bookmarks or instead of directly clicking on external links; they can find the site in the browser and check in the upper left corner whether it is safe. If it is safe, they can access it, and if not safe, they will not approach him (Kauffman, & Weber, 2020). With social network accounts with a high level of interaction with other accounts, external links can appear and receive in the inbox on the social network. This can reduce the risk of receiving such messages or links, but it cannot eliminate them. Therefore, it may be important not to open messages from unknown or suspicious accounts or, if there is such a possibility, to define a restriction or restriction on receiving messages from accounts that are not on the list of followers.

External links may contain a path to sites that have contagious material, which may allow attackers or unauthorised persons to access account information, which may include confidential and sensitive information and even in certain situations lead to permanent loss of access to the account. People who use accounts on social networks should pay additional attention to access devices that access a specific account on a particular social network. If, for example, the device does not have protected access via a password or some other form of protection, then another person who is not authorised to access the account can easily access it if you have a device that does not have a protection mechanism-specific social network. At the same time, it may be essential to pay extra attention to logging in to accounts through shared internet connections or shared devices. After using shared devices, it is necessary to delete any available trace of access to the account on the social network (Cram, Darcy, & Proudfoot, 2019). Shared internet connections can always be characterised as insecure or insecure. It is recommended to use different access passwords for other accounts on social networks. Suppose the same passwords are used for several accounts. In that case, an unauthorised person who acquires the password for one account can quickly obtain the password for other related accounts from the same owner. Passwords for accessing the account should be long and strong. Short sentences make the best passwords because they are easy to remember. For example, a string of three or more random words is as strong as a 10-character password that uses a mixture of numbers, letters, and symbols.

The main conclusion in this paper is that persons engaged in the social network account audit (Jakovljevic, 2021f) in each audit engagement should pay special attention to the information security of accounts as an essential segment of the social network account audit. The use of information that is the subject of sharing on accounts on social networks or are publicly available on them to create passwords to access the account may be considered undesirable. Attackers or unauthorised persons can quickly disclose this information. For example, if you share pictures of your cat online, make sure you don't use your cat's name as a password. Passwords should not be shared with anyone, not even children, parents or spouses. If there is a dilemma regarding whether all passwords will be saved, a password manager can be used to store and manage them (Anderson, Baskerville, & Kaul, 2017). Security and privacy settings need to be fully updated. You should never delay updates of this type on devices that access your account on the social network. Enabling two-factor authentication is another perfect way to protect social media accounts. For example, an application on a mobile phone that generates a unique code each time the login process is performed can access the account. This means that even if someone gets access to the account's passwords on the social network, if they do not have a mobile phone at the same time since the account is accessed, the account cannot be accessed on the social network. It should be borne in mind that everything you post online stays online, so you need to think before publishing any content.

LITERATURE

Anderson, C., Baskerville, R., L., & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems, 34*(4), 1082-1112.

Chung, N., K., Xiaojun, Z., James, T., Y., L., & Zan, T., K. (2021). Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. *Journal of Management Information Systems, 38*(3), 732-764.

Cram, W., A., Darcy, J., & Proudfoot, J., G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525-554.

Gattiker, U. E. (2013). *Social media audits: achieving deep impact without sacrificing the bottom line*. Chandos Publishing.

Ibnugraha, P., D., Nugroho, L., E., & Santosa, P., I. (2021). Risk model development for information security in organisation environment based on business perspectives. *International Journal of Information Security, 20*(1), 113-126.

Jakovljević, N. (2021a). Analiza osobina revizora. *SPIN21,* 366-374.

Jakovljević, N. (2021b). Analiza uticaja pandemije virusa Covid-19 kroz boravišnu taksu i stavove ispitanika. *Trendovi u poslovanju, 2*(18), 20-29.

Jakovljević, N. (2021c). Nepravilnosti u sprovođenju popisa imovine i obaveza. *Trendovi u poslovanju, 1*(17), 94-104.

Jakovljević, N. (2021d). Politička neutralnost u revizorskoj profesiji, stavovi ispitanika u Republici Srbiji. *BizInfo (Blace) Časopis za Ekonomiju, Menadžment i Informatiku, 12*(2), 23-38.

Jakovljević, N. (2021e). Primena digitalnih igara u revizorskoj profesiji. *SPIN21,* 374-382.

Jakovljević, N. (2021f). Upotreba dronova u revizorskoj profesiji. *SPIN21,* 382-390.

Jakovljević, N., & Jakovljević, J. (2021). Uticaj pandemije virusa Covid-19 na odgovornost revizora. *Finansije,* 92-113.

Jassim, N., A., Al-Zahir, B., A., M., & Khazraji, A., H., M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (iso/iec 27001:2013). *Journal of Management Information & Decision Sciences, 25,* 1-8.

Jingguo, W., Zhe, S., Gupta, M., & Rao., H., R. (2019). A longitudinal study of unauthorised access attempts on information systems: the role of opportunity contexts. *MIS Quarterly, 43*(2), 601-622.

Kajtazi, M., Holmberg, N., Sarker, S., Keller, C., Johansson, B., Tona, O. (2021). Toward a unified model of information security policy compliance: A conceptual replication study. *AIS Transactions on Replication Research, 7*(2), 1-15.

Kauffman, R., J., & Weber, T., A. (2020). Special Section: The Economics of Sharing and Information Security. *Journal of Management Information Systems, 37*(3), 598-601.

Kaušpadeiene, L., Ramanauskaite, S., & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological & Economic Development of Economy, 25*(5), 979-997.

Lin, W., Yang, C., Zhang, Z., Xue, X., & Haga, R. (2021). A quantitative assessment method of network information security vulnerability detection risk based on the meta feature system of network security data. *KSII Transactions on Internet and Information Systems, 15*(12), 4531.

Menard, P., Bott, G., J., & Crossler, R., E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems, 34*(4), 1203-1230.

Nasirpouri, S., F., & Biros, D. (2021). Understanding Employee Information Security Policy Compliance from Role Theory Perspective. *Journal of Computer Information Systems, 61*(6), 571-580.

Quesenberry, K. A. (2015). Conducting a Social Media Audit. *Harvard Business Review*, *18*, 1-6.