SECURITY RISKS ON SOCIAL NETWORKING WEBSITES

Dejan Vuletić, PhD, Assistant Professor[1]
Jovanka Šaranović, PhD, Research Associate
Strategic Research Institute, Ministry of Defence, Serbia

Abstract: This paper aims to provide a useful introduction to security risks in the area of social networking websites (social networks). A large number of users and the huge number of interactions are suitable for the rapid spread of malicious programs and spam, privacy breaches, identity abuses, frauds and other threats. This paper emphasizes the benefits of a safe and well-informed use of social networking websites. The paper presents the basic elements of the Guidelines for the use of social networks in the state administration, the autonomous province and local self-government in Republic of Serbia. The final part of the paper contains the consideration of social networking websites in military sector.

Keywords: social networking websites, users, security risks, public sector, army.

INTRODUCTION

Following a brief history of the Internet, we can see the development of a large number of virtual communities and groups around the world. With the appearance of the Internet, these communities in a very short time became truly global. Virtual communities are created with the advent of the Internet and new forms of communication, due to the basic need of the people for association, assembly and communication.

The advantage of communication innovation was first noticed by the academic population, leading to the establishment of the first social networks that were originally closed. The ease of use and the emergence of personalization features for profiles on portals, allowed users to present themselves, their interests, aspirations, thoughts, hobbies, etc.

The development of information technology has changed the way people communicate with each other, whereby in this communication mediated by computers and the Internet, as a global worldwide network. The most obvious sign of these changes is the creation of a fully interactive communication environment in a computer-mediated communication, created thanks to the flexibility of today's information technology. Distribution of this environment has created a completely new social environment, popularly called cyberspace. This social environment is a fertile ground for the creation of new social ties. Creating interactive media has enabled both individuals and community groups to direct discussions around common interests. In social environments, information is the basic medium of exchange that is available to the individual to build his/her cyber identity. Therefore, the information becomes a means of self-presentation and emotional presentation of the individual.[2]

1 E-mail: dejan.vuletic@mod.gov.rs.
2 Rheingold H., *The Virtual Community: homesteading on the electronic frontier.* 1993. http://www.rheingold.com/vc/book/

ABOUT SOCIAL NETWORKS

Online Social Networks or Social Networking Sites (SNSs) are one of the most remarkable technological phenomena of the 21st century.[3] Since the commercial success of an SNS depends heavily on the number of users it attracts, there is pressure on SNS providers to encourage design and behaviour which increase the number of users and their connections. Sociologically, the natural human desire to connect with others, combined with the multiplying effects of Social Network (SN) technology, can make users less discriminating in accepting "friend requests". Users are often not aware of the size or nature of the audience accessing their profile data, and the sense of intimacy created by being among digital "friends" often leads to disclosures which are not appropriate to a public forum. Such commercial and social pressures have led to a number of privacy and security risks for SN members.

Andreas Kaplan and Michael Haenlein define social media as a group of Internet applications that are built on the ideological and technological foundations of Web 2.0 technologies that enable the creation and exchange of user-generated content. Social media are media for social interaction and represent a kind of tools that go beyond the sphere of social communication.[4]

Bruce Lindsay, an analyst with the US Congressional Research Service (CRS) defines the social network as well as Internet applications as means allowing people to communicate and share resources and information.[5] Nicole Ellison and Danah Boyd define social network sites as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.[6]

Social network is a term for a form of human interaction in which through existing acquaintances meets new people to achieve social or business contacts. Web social networking sites allow users to meet new individuals from anywhere in the world without the need for actual physical contact. On the Internet, one can find several different social networks that offer different levels of interaction between the user's networks, depending on the amount of personal information that the user is sharing. The most popular networks of this type include Facebook, MySpace, Twitter and LinkedIn. On these social networks, it is necessary to create user profiles whereby requiring personal, sometimes sensitive information.[7]

Social network is possible to define as a web service that allows individuals to create a public (all users have access) or limited (only certain users have access to) personal profile in the system, create a list of acquaintances, browse and search list of acquaintances and others.[8]

The defining characteristics of an SNS are:[9]

- tools for posting personal data into a person's "profile" and user-created content linked to a person's interests and personal life,

- tools for personalised, socially-focused interactions, based around the profile (e.g. recommendations, discussion, blogging, organisation of offline social events, reports of events),

3 Hogben G., *Security Issues and Recommendations for Online Social Networks*, European Union Agency for Network and Information Security (ENISA), Heraklion (Greece), 2007, p. 2.
4 Kaplan A., Haenlein M., *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, Vol. 53, Issue 1. Kelley School of Business, Indiana University, 2010, p. 61.
5 Lindsay B., *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, *CRS Report for Congress*, Congressional Research Service, 2011, p. 1.
6 Ellison N., Boyd D., *Social Network Sites: Definition, History, and Scholarship*, Journal of Computer-Mediated Communication 13, The Pennsylvania State University, 2008, p. 211.
7 *Sigurnosni rizici društvenih mreža*, Hrvatska Akademska Istraživačka mreža – CARNet, Zagreb, 2009, p. 1.
8 *Ibid*, p. 5.
9 Hogben G., *op.cit*, p. 5.

- tools for defining social relationships which determine who has access to data available on SNSs and who can communicate with whom and how.

SNSs may be seen as informal but all-embracing identity management tools, defining access to user-created content via social relationships. The value of SNSs lies not just in the content provided (which is group-specific), but in its replication in electronic form of the web of human relationships and trust connections.

The success of some social networks depends on the number of users who can use functions that the network offers. However, with the number of users of a social network increasing, the financial value of the social network is growing, which allows the owner of the network expansion of marketing solutions available on the social network.[10]

Being a user of social networks has certain advantages such as a sense of connection with other individuals, meeting like-minded, new way to share life experiences and scientific discoveries, and controlling the amount of personal information that will be displayed on a social network (which in other forms of social media, such as blogs, is not possible). Ability to manage the amount of personal information on a social network is certainly an advantage, because the user chooses what personal information to reveal and thereby protect their privacy. Users are often not aware of the number of individuals who have access to their personal information. User data are often not adequately protected, resulting in security incidents occurrence and abuse of personal data. Social networks are becoming a worldwide phenomenon. Social networks provide users with an easier way of communication, the opportunity to meet new people and exchange of data. The original social network on the Internet did not have a large number of functions, so the number of security incidents was minimal.[11]

The success and popularity of some social networks depend on adapting to users' needs, as well as setting up of new technologies in order to attract new customers and retain existing ones. Some social networks have achieved great success when it comes to the number of users because of the ability to quickly adapt.[12]

THREATS IN SOCIAL NETWORKS

Communication on social networks has many advantages, but carries with it certain risks. Attackers may compromise the privacy of users in many ways. Most social network users inadvertently reveal much information to attackers. In order to start new friendships with strangers, users reveal personal and sometimes sensitive information, which in some cases can pose a security risk. It is believed that the greatest damage to the users of a social network can cause programs by unknown authors containing personal questions that the user should respond. Unaware of the danger of such programs, they are forwarded to users in the list of friends, who again after completing the programs are sent to users from the list of friends, and so on.[13]

Fake profiles are not required to have a malicious effect, however, if it is their purpose, can cause considerable damage to persons whose identity is used. The risks of fake profiles are: damage to the reputation of individuals, blackmailing individual, use of false profile to incite other users to disclose personal and confidential information and marketing activities through fake profiles.

Cyberbullying is a term used to describe the harm to another individual by means of tech-

10 *Sigurnosni rizici društvenih mreža*, *op.cit.*, p. 1.
11 *Ibid*, p. 5.
12 *Ibid*, pp. 9–19.
13 *Ibid.*, pp. 9–19.

nology, usually using the mobile phone or through the Internet. Usually there is a modified multimedia (photos, videos, etc.) that aim to humiliate the individual, and degrading messages and comments on someone's user profile.

The best-known security flaw on Facebook is caused by improper handling ActiveX controls for uploading photos (Facebook Photo Uploader) on the user's profile. When one tries to upload photos to the profile, he/she is given a warning that it is necessary to incorporate an additional ActiveX control in order to upload the desired photos. If the user has agreed to install a malicious ActiveX control on his/her computer, there is a possibility that an attacker takes control of the user's computer, and executes arbitrary code. This failure was resolved in a short period of time.

Also, there have been several cases on Facebook where an unknown attacker managed to get the users' names and passwords for specific members, and thus compromise the privacy of the data stored in the profiles. Customer safety has also been severely compromised by the appearance of worms Net-Worm.Win32.Koobface.b. It is known that the worm spreads via spam, and modifications to Facebook resulted in automatically sending spam messages to users on a compromised account's friend list.

The dialog box appears on the screen, telling the user to install Flash program on the computer to stream media content, which then infects the user's computer with the worm Koobface. The attacker will then use the infected computer to further spread malicious software or carry out other forms of attack.

Among the best known security vulnerabilities on the network Twitter is a flow relating to allowing the execution of certain code on someone's profile. The mentioned security flaw is used by a worm named "StalkDaily". The worm "StalkDaily" quickly expanded on Twitter. The user could infect profile simply by viewing the profile of another user who is infected with malicious software.

Also, one of the attacks on the Twitter is caused by insufficiently good authentication to the network. A hacker named "Hacker Croll" was able to detect the user name and password of an administrator of the Twitter, and was able to endanger the safety of millions of users. A hacker broke into the mailbox of the administrator and then found the username and password for Twitter. As evidence for the above mentioned actions, the hacker provided a screenshot of the administrator's account and warned the owners of Twitter of insufficiently good authentication procedures for administrator accounts. Possible protection against these attacks is the use of two or more factor authentications when logging in to the administrator account.

A security vulnerability of LinkedIn was discovered in LinkedIn's add-on for the Internet Explorer. Using spam messages, the attacker could mislead users to visit a malicious page and download malicious program code. Because of flaws in ActiveX controls of the said tool, the attacker could take control of users' computers or execute DoS (Denial of Service) attack. Security flaw in LinkedIn's add-on for the Internet Explorer has been corrected.

Similarly to other networks, the most common attacks are spam messages and directed phishing attacks (spear phishing attack). LinkedIn users often receive emails from network administrator or other users of the network. In this case, the attacker sent spam e-mail messages on the e-mail addresses of 10,000 LinkedIn users that appeared to have been sent by the network administrator. However, the specificity related to phishing attacks is that the attacker was sending spam messages that might interest the user. Thus, the attacker has previously managed to find out personal information about users to which the spam message will be sent. In this case, the spam messages contained a link to a malicious site, which infected users with a malicious program. The attacker could then gain access to the users' computer, and compromise the privacy and safety of users.

According to Hogben Giles, main threats on social networks are:[14]

- Digital dossier aggregation.
- Secondary data collection.
- Face recognition.
- Content-based Image Retrieval (CBIR).
- Difficulty of complete account deletion.
- Spam.
- Cross site scripting (XSS), viruses and worms.
- Spear phishing.
- Infiltration of networks.
- Profile-squatting and reputation slander through ID theft.
- Stalking.
- Bullying.
- Corporate espionage.

The same author gives some recommendations for reducing threats:[15]

- Encourage awareness-raising and educational campaigns.
- Review and reinterpret the regulatory framework.
- Increase transparency of data handling practices.
- Discourage the banning of SNSs in schools.
- Promote stronger authentication and access-control where appropriate.
- Implement countermeasures against corporate espionage.
- Maximise possibilities for abuse reporting and detection.
- Set appropriate defaults.
- Providers should offer convenient means to delete data completely.
- Encourage the use of reputation techniques.
- Build in automated filters.
- Require consent from data subjects to include profile tags in images.
- Restrict spidering and bulk downloads.
- Take the measures of protection from spam and phishing.
- Promote and research image-anonymization techniques and best practices.
- Research into emerging trends on social networks.

SOCIAL NETWORKS IN THE STATE ADMINISTRATION, AUTONOMOUS PROVINCES AND LOCAL SELF-GOVERNMENTS OF SERBIA

The bodies of state administration, autonomous provinces and local self-government, (public administration), as the citizens' service, in order to establish regular, rapid and transparent communication with the public and provide information about the work of public

14 Hogben G., *op.cit.*, pp. 3–4.
15 *Ibid.*, pp. 4–5.

administration and independent institutions, should create an interactive and proactive communication on social networks.[16]

The development of social networks (Facebook, Twitter, LinkedIn, etc.) on the Internet has changed the way of communication and content sharing. The users come to more content through social networks compared to traditional search via search engines or accessing the web sites. In order to increase the availability of published information, it is necessary to maintain a web presence, adapt to quick and easy sharing of content on social networks using web technologies that allow this. In this regard, it is recommended to share content that changes on a daily basis (news, current affairs, events, activities, etc.).[17]

The main features of social networks is that they are the most effective and quickest source of information, are transparent, always available, free, public, dynamic, multimedia, and provide the necessary two-way communication. When most government agencies use social networks as a tool for communicating with citizens and keeping them informed, it would undoubtedly lead to greater confidence in the operation of the state. There is no doubt that fast, accurate and continuous information provided to the citizens, leads to increased trust, which creates a positive attitude towards a state agency, which is a good way of representing and communicating with citizens on social networks.[18]

Most people using smart phones spend a lot of time browsing Facebook or content of some other popular social networks. According to research of the Republic Agency for Electronic Communications on the number of sold phones and SIM cards, it can be concluded that every citizen of Serbia has two mobile phones. Another important consideration in the decision on opening an online account is the possibility of referring to the development of mutual relations of trust between state institutions and Internet users.[19]

Timely, clear and direct communication with citizens will reinforce the impression of an efficient and transparent work of state institutions. On the other hand, avoiding the usual technical terminology which is sometimes incomprehensible for the citizens and the use of simple everyday language, will bring state institutions closer to the Internet users and will help consolidate the relationship of trust and understanding.

One of the many advantages of social networks consists of the fact that when one wants something to suggest to the public and is not sure what the reaction will be to it, it is recommended to first communicate on social networks. This provides several things – primarily allows people who understand the scope of work of national authorities to directly participate in the creation of something new, and the authorities get the opportunity to see and hear what it is that citizens and businesses need. Since the job of the state is to help citizens and ensure smooth operation of businesses, appropriate authorities, via social networks, can see what they need to change to facilitate daily operations.

Finally, it is important to note that any form of communication, being it internal or external, belongs to the public relations. The way of communications with citizens and the public must be such as to give the impression that the institution is willing to listen to and acknowledge everyone's opinion.

16 *Guidelines for the use of social networks in the state administration, the autonomous province and local self-government*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2015, p. 4.
17 *Guidelines for creating web presentation of state administration, territorial autonomy and local governments v. 5.0*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2014, pp. 10–11.
18 *Guidelines for the use of social networks in the state administration, the autonomous province and local self-government*, *op.cit.*, p. 4.
19 *Ibid*., p. 5.

SOCIAL NETWORKS IN THE ARMY

Social networks at the same time could be used for defence activities (prevention, warning, forecasting, institutional communication, crisis management) and for offensive action (influence, propaganda, deception).[20]

By using Internet-based platforms like Facebook and Twitter, social media provides new ways to connect, interact and learn. Social media, with a variety of available platforms, can instantaneously connect users within a global network, making the transfer of information even more pervasive. Today, social media is so widespread and transparent that one may already be involved even if not actively participating. Social media is highly effective tool to use when reaching out to large communities and audiences. But with this substantial ability to connect with the masses, comes risk. Using social media to spread information is becoming the standard. More and more units are using social media to communicate, so it's more important than ever to understand the risks associated with using the various platforms.[21]

The Army understands the risks associated with social media and has worked hard to develop training to help soldiers and family members use social media responsibly. Soldiers using social media must abide by the Uniform Code of Military Justice (UCMJ) at all times. Commenting, posting, or linking to material that violates the UCMJ or basic rules of soldier conduct is prohibited. Social media provides the opportunity for soldiers to speak freely about what they're up to or what their interests are. However, soldiers are subject to UCMJ even when off duty, so talking negatively about supervisors, or releasing sensitive information is punishable under the UCMJ. It is important that all soldiers know that once they log on to a social media platform, they still represent the Army.[22]

When using social media, soldiers must avoid mentioning rank, unit locations, deployment dates, names, or equipment specifications and capabilities.[23] Geotagging photos and using location-based social networking applications is growing in popularity, but in certain situations, exposing specific geographical location can be devastating to Army operations. While soldiers are engaged in Army operations, they should turn off the GPS function of their smartphones. Failure to do so could result in damage to the mission and may even put families at risk.[24]

Soldiers cannot include any copyrighted or trademarked material on their social media platforms. Social media is about connecting, so it is only natural that Army leaders may interact and function in the same social media spaces as their subordinates. How they connect and interact with their subordinates online is up to their discretion, but it is advised that the online relationship function in the same manner as the professional relationship.[25] If a leader comes across evidence of a soldier violating command policy or the UCMJ on social media platforms, then that leader should respond in the same manner they would if they witnessed the infraction in any other environment. Using rank, job, and/or responsibilities in order to promote oneself online for personal or financial gain is not appropriate. Such actions can damage the image of the Army and an individual command.[26]

By watching the wall on a Facebook site, or by reading the comments on a blog post, social media managers can get a feel for what the online community wants to hear about. Some-

20 Montagnese A., *Impact of Social Media on National Security*, Centro Militare Di Studi Strategici, Rome, 2012, p. 21.
21 *U. S. Army Social Media Handbook,* Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2011, p. 3.
22 *Ibid.*, pp. 3–4.
23 *Ibid.*, p. 5.
24 *Ibid.*
25 *Ibid.*, p. 11.
26 *Ibid.*, p. 6.

times, it is useful to talk to an audience directly. Ask for feedback and suggestions, and then act on that feedback. A social media presence accomplishes very little if the online audience is not interested in what's being said. Listening to an audience can mean the difference between maintaining a successful social media presence or an irrelevant one.[27]

Using social media to communicate with stakeholders during a crisis has proven to be an especially effective due to its speed, reach and direct access. In recent crisis, social media has helped distribute command information to key audiences and media while also providing a means for dialogue among the affected and interested parties.[28]

The Army recognizes that social media gives people the ability to communicate with larger audiences faster and in new ways. It has become an important tool for Army messaging and outreach. The Army understands the risks associated with social media and has developed training to help soldiers and family members use social media responsibly.[29]

Most of social media failures can be attributed to organizations rushing into social media before determining what exactly the organization aims to achieve with social media platforms. Using social media effectively is a process and it requires strategy, goals, manpower and foresight. By reading the comments on a Facebook wall or blog post, social media managers can get a feel for what the online community wants to hear. It is also useful to talk to your audience directly.[30]

Social media sites provide their own free analytics tools that allow administrators to track views, impressions and comments. By using numbers in conjunction with comments and reader feedback, it is easier than ever to determine how organizational messages are received and how the audience is responding to the content. Some analytics tools provide graphs and charts, but ultimately the presentation of information depends on the platform. These different presentations make for a richer statistical analysis. Using free analytics tools can help a unit demonstrate the usefulness of a social media platform, and even highlight the success of a specific social media campaign.[31]

Keep your social media presences up-to-date by using mobile devices, if necessary. The myriad of mobile devices available today allow you to update social sites without being tied to your computer at a desk. Crisis happen all the time, so be prepared. Whether the installation is on lockdown, you're waiting out a storm or you're at a remote site at the scene, mobile devices allow you to share updates immediately. Ensure your mobile devices are continuously charged and be creative in finding power solutions that work for your situation.[32]

Social media is becoming a valuable tool for keeping families and soldiers connected, which is vitally important to unit well-being.[33] The Department of Defence specifically encourages service members and their families to use social media. Social networking sites provide a safe space for individuals to share their problems with others and to receive advice from others while maintaining a comfortable emotional distance. Social media also affords users tremendous opportunity to exchange information in a rapid, efficient, low-cost manner. Research is mixed regarding the power of social media to connect people or isolate them, and to alleviate or exacerbate stress. It is likely that a range of outcomes may be associated with social media use depending on a wide range of factors.[34]

27 *Ibid*, p. 9.
28 *Ibid*., p. 10.
29 *U. S. Army Social Media Handbook (version 3.1)*, Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2013, pp. 1–2.
30 *Ibid*., p. 5.
31 *Ibid.*
32 *Ibid*.
33 *Ibid*., p. 19.
34 *Social Media Communication with Military Spouses*, The Military Reach Team, The University of

CONCLUSION

Social networks are a phenomenon that in the past decade spread rapidly and globally. Social networks have changed the way of communication, the daily activities of people, and in a way, changed the world. Social networks are communication tools and they can be a threat or an opportunity for national security.

Social networks made a major shift in communication in the public sector, the army, the business area. With the advent of technologies that use social networks, new vulnerabilities that attackers could exploit will appear.

Users of social networks should definitely pay attention to threats which can endanger large amounts of personal or confidential information. By using anti-virus, anti-spyware tools and similar mechanisms for the protection and application of precautions when using social networking, users will primarily provide privacy for data that will not be disclosed to anyone.

That is why wider adoption of the national strategy of social networks is very important. According to Macnamara, a small number of government agencies and institutions in the world has adopted a national strategy to deal with the proper use of social networks.[35] The lack of strategy for social networks presents large national security risks.

The future of social networks is hard to predict, but there are still some limits that can be moved in order to achieve even better communication among users. The idea is emerging as the next major shift in communication via social networks is the possibility of communication between users of different social networks. Also, it is expected that the created user profiles on social networks will be able to install other web services, applications, etc.[36]

REFERENCES

1. Ellison N., Boyd D., *Social Network Sites: Definition, History, and Scholarship*, Journal of Computer-Mediated Communication 13, The Pennsylvania State University, 2008.
2. *Guidelines for creating web presentation of state administration, territorial autonomy and local governments v. 5.0*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2014.
3. *Guidelines for the use of social networks in the state administration, the autonomous province and local self-government*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2015.
4. Hogben G., *Security Issues and Recommendations for Online Social Networks*, European Union Agency for Network and Information Security (ENISA), Heraklion (Greece), 2007.
5. Kaplan A., Haenlein M., *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, Vol. 53, Issue 1. Kelley School of Business, Indiana University, 2010.
6. Lindsay B., *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, *CRS Report for Congress*, Congressional Research Service, 2011.
7. Macnamara J., *Social Media Strategy and Governance - Gaps, risks and opportunities*, Australian Centre for Public Communication, University of Technology, Sydney, 2011.

Minnesota, Minnesota, 2015, pp. 4–13.
35 Macnamara J., *Social Media Strategy and Governance - Gaps, risks and opportunities*, Australian Centre for Public Communication, University of Technology, Sydney, 2011, p. 2.
36 *Sigurnosni rizici društvenih mreža*, *op.cit*., p. 26.

8. Montagnese A., *Impact of Social Media on National Security*, Centro Militare Di Studi Strategici, Rome, 2012.

9. Rheingold H., *The Virtual Community: homesteading on the electronic frontier.* 1993.http://www.rheingold.com/vc/book/

10. Sigurnosni rizici društvenih mreža, Hrvatska akademska istraživačka mreža – CARNet, Zagreb, 2009.

11. Social Media Communication with Military Spouses, The Military Reach Team, The University of Minnesota, Minnesota, 2015.

12. U. S. Army Social Media Handbook, Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2011.

13. U. S. Army Social Media Handbook (version 3.1), Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2013.