Investigation of social media security : A Critical Review

Article *in* International Journal of Architectural Computing · August 2020

CITATIONS
0

READS
4,439

2 authors, including:

W. Sanduni Shashipraba Perera
Sri Lanka Institute of Information Technology
7 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Investigation of social media security : A Critical Review

Shashipraba Perera
Department of Information Technology
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
shashipraba.56@gmail.com

Hiruni Fernando
Department of Information Technology
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
fernandohiruni55@gmail.com

***Abstract*— The utilization of social media security is now a topic that is discussed widely. People still do not seem to have a concern about security of social media. In this current literature critical review, we are discussing some of the most important qualitative studies that explore and research about the use of social media security. Social media includes a wide range of websites and apps like Twitter, Facebook and Instagram. All the social media connect with each other and exchange information, so users should be mindful of the drawbacks and impacts of using social media sites. We consider the history of social media and the need of social media to highlight the background social media's background. Then we address the social media's idea security and the social media security risks with the challenges. We conclude with a discussion of potential steps for future of social media security/ possible solutions for security.**

Keywords*— *Social media, OSN, social media security, classic privacy threats, modern threats

I. INTRODUCTION

Social media is known as a mutual term for websites and applications. This is mainly focus on communication, community-based input, interaction, content-sharing, and collaboration. There are different other types of social media. This is dedicated for forums, microblogging, social networking, social bookmarking, are among them.

Social media takes a major role in the present society. People enable them keep to be connected with each other in a better manner and make new opportunities for their business. In the present, many people are using social media in a high percentage. Recently, the internet is the most growing technology for almost everyone's everyday uses. With Internet technology, everyone around the world can communicate, exchange information, play, and many other Internet uses in a simple and semi-free manner, even with very limited information technology experience [1]. Social media is a series of Web pages focused on the Internet. Social media's purpose and the role is to facilitate the personal as well as business-focused engagement people of around the world. Social networking is a tool that enables content sharing between users. The contents are different types of information on a range of topics. In addition, the service also helps users to exchange new concepts, thoughts, and experiences with many people. Many social media forms, networks and services are available nowadays, including Facebook, Instagram, YouTube, LinkedIn, Twitter, and snap chat [1].

Social media networks like Twitter, Facebook, snap chat, Instagram, YouTube have seen a dramatic increase in the number of users over the last decade. It is because it is popularly affect as a means of communication, sharing information and thoughts, and attract more and more people through many other features around the world, particularly with the use of smartphones. Sites of social networking can be useful resources for sales and promotions as well as enjoyable amusements.

The 2019 global digital survey, which reveals that in 2019 the amount of web users worldwide was 4,388 billion, while in 2019 the number of social media users in around the world was 3,484 billion, in 2019 number of cell phone users was 5,112 billion [1]. Some of the fascinating things the global digital study found was that social media usage increased by 9 per year, while the number of internet users increased by 9.1 per year [1].

Today, almost everybody in the world uses social media but most of them do not always give concern to security. This is the procedure of analysis of social media dynamic data to save from ultimatum in business. Every industry has to face some sort of a special collection of risks on social. Many put themselves at the center of controversy or in the press of the organization. In the present, many people are using social media in a high percentage. They did not consider their data and information security. In the present time, Social media networks are always the main priority target of cyber security attacks. Because of their massive user base. There are many studies that explore vulnerabilities of security as well as issues of privacy in social networking sites. Those researches made better recommendations to diminish from security risks. Therefore this analysis focuses mainly on factors of study impact among users of public sector organizations for the protection of social media emphasis. Particularly in the education sector.

In current times many people are using social media. Every social media application asking personal details for signup. Every people give their all details depends with their privacy without considering whether they are using is more secure or less secure. Here is the breakdown of personal information that all social media platforms are gained by users. Name, email, address book, credit card information, debit card information, language, etc. There are couple of tools in security tools. They are social media developers realized security tools and external web services realized tools. The combination of those two tools allow for a user to complete the security of accounts. There are some of them as an example; two-factor authentication, private account, security checkup, login notification, password strength

checker, trusted contacts, periodic password changes, external application or site access checkup, email breaches checkup, identification code etc. [2].

This paper is structured as follows; Section 1 is an introduction of the topic of the review paper, 'investigation of social media security' presenting the study's objectives and issues that those prominent studies have examined in order to achieve these objectives. In Section 2, researchers provide readers the related literature pertaining to social media security, beginning from its history and evolution. There researchers' aspects related to social media history are reviewed. This will be very helpful and useful for people who are unfamiliar with social media's beginning and the development of industrialization. In the same section next, going through a brief introduction of the need of social media. Then the role of Security in Social media and need of security in social media are reviewed. Social media security risks, social media challenges and opportunities are then discussed. Finally that section ends with the future work and possible solutions. Section 5 is reserved for analysis and discussion of the studies or papers followed for this review. The researchers will focus to identify the important parts of the studies and the research gaps of the referred papers, from that information. Lastly, Section 7 is a conclusion to the review paper by specifying the important findings from the studies and papers discussed in this review.

II. LITERATURE REVIEW

A. History and Evolution of Social Media

The use of the internet started to spread and people experiences new life since 1980 [4]. Social media comprises communication websites that facilitate relationship forming between users from diverse backgrounds, resulting in a rich social structure [8]. More specifically [7] define social media as Social media is a means of contact for online interactions between the end users (viewers) and data generators (data owners) who build virtual communities using online social networks (OSN) [7].

B. Need of Soial Media

Why do we need social media? Social media accept a bond building between users from distinct backgrounds, resulting in a tenacious social structure [8]. However, according to [5] currently websites of social networking have become an active ground for cybercriminals. So does social media have positive or negative effects? According to [7] Social media is one form of communication which has both positive and negative effects for its users [7]. This study has been able to convey both positive and negative effects of social media to users clearly.

C. Access and usage of Social Media

In general, users may use their personal computers or mobile devices to access social media services through web based technologies [1]. Such accesses to websites of social media allow users to have an account or build their own accounts through some authentication and compliance with policies. The verification involves special information about an individual, such as a telephone number, email address, current location, etc. On the other hand, the social media policy's aim is to set standards for acceptable actions and ensure that users do not expose social media platforms to legal or public humiliation issues.

These regulations include guidelines on using the platform for social networking, and guidelines on what kinds of knowledge should be exchanged. Nearly all social media policies contain limits on disclosure of sensitive or proprietary company information or something that could influence others. The incorrect use of social media, particularly users who have no or limited cyber culture, may face the user to attack or hack.

About 3.48 billion active social media users now exist, making social media an inevitable part of life strategy [1]. Social media network users can share various pieces of personal information with others when people upload their images, share their birth date, reveal their phone number and write their current address. Sharing such personal data will lead to misuse of the data. For example, some users exchange profile information that includes their full name, telephone number, and other sensitive details. Hacking uses one of the users ' social network account and the hacker can misuse the information for blackmailing the user.

While comparing the most popular social networks, it's important to evaluate them by active account usage, not just by the number of user accounts. Research has shown that some social networks are rising faster than others, although others are in decline now. Popular examples of social media sites are Facebook, Twitter, Instagram, etc.

Nowadays, Facebook is one of the most popular social media in use around the world. In 2019, Facebook announced that they have more than 2.38 billion active monthly users [1]. The network enables users to create profile pages where they can view themselves, post photos etc. Facebook also allows various apps to be used inside the network, from fortune cookies to messenger. Twitter is a microblogging website and up to one hundred forty characters of short messages may be added to her or his account.

Instagram is a popular service to the social media network. Messages and ideas are exchanged between people in these media networks. In such a media network photos and videos are shared primarily. This provides simple video integration and is therefore frequently used by any single user to show their own ideas.

D. Role of security in social media

One of the biggest disadvantages of social media is the issue of privacy and security. But why exactly we need security in social media. In spite of the security of social media is a now widely-studied subject, there still does not seem to be a consensus for exactly why we need social media security. It was checked that most consumers are generally unaware of the fact that the numerous privacy risks involved in posting personal information on social networking websites are widespread. [5]. But [7] has mentioned that, Social media prominence is such that active social media users around the

world are projected to reach some 2.95 billion by 2020 [7]. However, there's quite less information on why social media security is needed in this paper.

E. Social media challenges, security risks and opportunities

Users exchange a huge amount of personal details on social networks, making them a target for different types of Internet attacks, including identity theft, phishing, cyber bullies, spamming, Web fraud, etc. Social networks provide hackers with vast opportunities to rob identity. In these types of attacks, a malicious individual may steal his or her personal details, including bank accounts, addresses, telephone numbers, etc., without the user's permission, and using it to commit cyber-crime. For example, a lot of social networks, including Facebook, give their users game apps [3].

To complete the registration process, such applications include personal details, like the user's credit card details, phone number, email, etc. Of course, when a user shares the phone number and credit card details the risk of personal details theft and phishing attacks is increased. In certain cases, apps that result in the user resorting to redirect the user's attention to harmful content and damage its credibility.

Some of the most obvious potentially innocuous possibilities in the sense of social networking may be the illegal use for promotional purposes of personal details, the collection of possible friends or the discovery of content that may be of interest. Such techniques are considered a common process within social networks, and everybody knows about the collection, review, and usage of personal information for various purposes, including commercial usage. For one thing, it has already verified the transfer of personal data from different social networks.

One of the main issues for users is that numerous user specific data leakage can be observed as a consequence of the social network's failure within the framework of various initiatives. One causes of significant disruption is hacking user accounts or lack of accountability, and intercepting all personal information. When the problem is huge, there will be more serious issues. There are several possible risks to users, like computer bugs, malware, Trojan horse, phishing, and other malicious software, and they can be used to steal sensitive information from the user.

According to experts, phishing attacks are one of the most common cybercrime attacks and the key focus is Internet payments, Internet banking, Internet stocks, online games, Web 2.0 technology used pages, and so on [3]. Beyond the danger of misuse of personal details, social networks are an instrument for mass demonstrations in the sense of threats to public security. The disruptive problems of social networks are revealed to outside intervention, creating tensions between the government and the people, demonstrations in a short time.

The research [4] uses a web-based survey to define the relationship between security expectations of users and their actual actions on social media. .But as mentioned in the topic the results of the IT students' perceptions are not clearly highlighted.

Online users have been exposed to security and privacy threats because of the high usage of social media [4]. Such threats can be classified into modern threats and classic threats [4]. Modern threats are related to users of social media only because of the architecture of social media which can compromise user safety and privacy. Classic threats are cyber threats that make social media users as vulnerable as well as other internet users that don't use any social media. However, in [6] the threats are arranged into Privacy related threats and traditional network threats. This categorization does not provide clear examples for the privacy related threats.

This is the technique by which the user's identity is stolen and is known as profile cloning [5]. But according to [7], Cloning profiles can be done by an attacker using theft credentials from an existing profile, generating a new fake profile by using private information stolen [7]. The last mentioned brings out the clear definition of what is profile cloning.

F. Some possible solutions and Future work

Social media have different variety of privacy and protection concerns, but using precautionary steps can help users overcome the privacy challenges. Users are careless and this leads to attackers to exploit privacy and security issues in social media. So sometimes the content shared with other users can go into the wrong hands, either in the same format or in another way. However, the frontline protection against these threats to privacy is given through the privacy settings regulated by OSNs [7].

The security level of social media accounts is linked to the server-side collection of information protection tools built by the social media developers and some additional external security tools that a user would use on a regular basis [2]. The combination of these two types of security tools helps a user to completely configure account security: Two-factor authentication is a security function that, in addition to a password, helps secure user account. Two-factor authentication uses two factors to authenticate an individual. The private account where all posts are private and only approved followers may access posts. Login notification is a security function that notifies users of new account logins. Security check-up allows authorized devices to be checked. Therefore, no need to enter a verification code every time you sign in with trusted devices.

Trusted contacts feature that allows you to pick from your friend list three to five confidants to obtain a virtual key to your social media account. Identity code is a protection mechanism that produces an identification code that can be used to authenticate two factors. A password strength checker allows users to check the password power. A password breaches checker ensures that password infringements can be identified. It is recommended that a password be updated if it is in this web-service. E-mail breaches checker is a monitoring tool that enables the email breaches to be revealed. An e-mail will be updated if it is in this web-service database.

But in contrast [9] points out a different solution. The amount of personal information posted should be limited, and not post home addresses or private contact information [9]. Furthermore, there are more solutions discussed in the study [9] compared to other papers. Do not use applications from third parties which often find their way around Facebook. Often they install malware that monitors the online activities. Use clear passwords, use anti-virus tools, and keep the applications up-to-date to help protect against current security threats. They need to be closely monitored for those with children because they sometimes don't know the wise online protection strategies or are careless to be protected [9].

There are some new solutions proposed as well as future works regarding social security. The biggest problem here is carelessness in what is posted online, and this is one of the easiest to solve conceptually [9]. Protection motivation theory (PMT) has been widely used for analyze the actions of people in the area of information security. The research mentioned in [4] proposes that PMT theory can also be applied to clarify and predict behaviors of social media users with implications for protection. Even Though, the idea of the solution had some missing areas the paper extended the PMT application to social media. However, this study examines the relationship between user expectations of protection and their actual activity on social networking sites using Facebook as our survey platform [4]. The study found that expectations of users regarding activity with security consequences have no substantial connection with the probability of doing this behavior. More researchers will consider investigating behaviors that have security consequences on social media networks [4].

II. ANALYSIS AND DISCUSSION

In [4] the topic is very significant but the paper has not highlighted the IT student's perception exactly as mentioned in the title. The abstract clearly describes the objectives and the methodology that is going to be followed to assess the security knowledge of users on social networking sites and to gather data about their actual actions. But the results obtained have not been mentioned in the paper.

In [5] the abstract is quite long and presents a detailed introduction. But the objectives and results obtained are described accurately.

In [2] Two-factor authentication is the most important of the social media security mechanisms and the least important of these is identity codes generation. The average value calculated for the degree of social media security is 91.4.

Third-party software or apps are expanded functionality that social networking sites providers may deliver to encourage users to stick with their social networking sites. To order to use such devices, users must allow software developers to access some of their personal information, who then have complete rights to monitor the personal information of the user. In 2007, Facebook started to incorporate the third-party application feature and most other social networking sites require access to the social graphs of their results. Nonetheless, most users rely on providers of social networking sites to protect their personal data. User personal data accessing third party applications were ultimately migrated to a third-party server.

Thus, service providers and software developers rely on each other for their own benefits. Hence the confidentiality of the user's personal information is not well covered and can also be leaked.

Although, several studies have addressed common attacks and problems, some researchers have carried out vulnerability tests or created new models of attacks to assess the strength of the system and to check for system vulnerabilities or weaknesses.

III. CONCLUSION

Through all these research works it is very clear that social media includes high-security risks as well as risks to privacy. Because of their centralized infrastructure, their massive archive of all the personally identifiable data a hacker could ever need, and the general public's ignorance of how to properly use privacy settings to improve their online security [9], they run this danger. There is also a huge danger, because a lot of people, especially adolescents, always tend to trust other people quickly. So, they become extremely confident about others. Not only that they also share private details about themselves without a proper understanding of what kind of details they should share about themselves online.

Social media have some benefits, but in addition to these advantages, OSN's posed some similar concerns. Users' privacy and protection, and their information, are key issues in social media [4]. While there is some general opinion about what social media security and what it can help the online users, there are still many unanswered questions. We think that the headway of new technology as a rule and specifically, social sites will bring new security risks which may open the doors to vindictive performers, key lumberjacks, Trojan horses, phishing, spies, viruses and attackers [6]. However, there are many possible solutions presented to avoid the risks. Information security experts, government officials, and other intelligence officers need to develop new strategies that combat and adjust to the emerging future risks and threats [6]. Moreover in the technical aspect, for preserving the security of social media, techniques like K-anonymity and diversity can be used [5].

REFERENCES

[1] S. R. Zeebareea, S. Y. Ameen and M. A. M. Sadeeq, "Social Media Networks Security Threats, Risks and Recommendation: A Case Study in the Kurdistan Region," 2020. [Online]. Available: https://www.researchgate.net/publication/342693220_Social_Media_Networks_Security_Threats_Risks_and_Recommendation_A_Case_Study_in_the_Kurdistan_Region. [Accessed 02 August 2020].

[2] R. Shevchuk and Y. Pastukh , "Improve the Security of Social Media Accounts. 439-442. 10.1109/ACITT.2019.8779963.," 2019. [Online]. Available: https://www.researchgate.net/publication/334891408_Improve_the_Security_of_Social_Media_Accounts. [Accessed 02 August 2020].

[3] R. Alguliyev, R. Aliguliyev and F. F. Yusifov, "Role of Social Networks in E-government: Risks and Security Threats.," Online Journal of Communication and Media Technologies., 2018. [Online]. Available: https://www.researchgate.net/publication/328896849_Role_of_Social

_Networks_in_E-government_Risks_and_Security_Threats. [Accessed 10 August 2020].

[4] Z. Y. Alqubaiti, "The Paradox of Social Media Security: A Study of IT Students' Perceptions versus Behavior on Using Facebook.," [Online]. Available: https://www.researchgate.net/publication/313566403_The_Paradox_of_Social_Media_Security_A_Study_of_IT_Students'_Perceptions_versus_Behavior_on_Using_Facebook. [Accessed 09 August 2020].K. Elissa, "Title of paper if known," unpublished.

[5] P. Goud Kandikanti, "Investigation on Security Issues and Features in Social Media Sites (Face Book, Twitter, & Google+)", 2017.

[6] S. Kumar and V. Somani, "Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques.," 2018. [Online].

[7] I. Ud Din, N. Islam, J. Rodrigues and M. Guizani, "Privacy and Security Issues in Online Social Networks," 2018. [Online]. Available: https://www.researchgate.net/publication/329118582_Privacy_and_Security_Issues_in_Online_Social_Networks/citation/download. [Accessed 15 August 2020].

[8] K. K. Kapoor, K. Tamilmani, N. P. Rana2, P. Patil, Y. K. Dwivedi and S. Nerur, "Advances in Social Media Research: Past, Present and Future," November 2017. [Online]. [Accessed 18 August 2020].

[9] D. Hiatt and Y. B. Choi, "Role of Security in Social Networking," 2016. [Online].

[10] A. . E. Waldaman, "Privacy, Sharing, and Trust: The Facebook Study." Case Western Reserve law review 67 (2016): 193.," 2016. [Online].