International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.21, June 2019– www.ijais.org

Risk Measurement Models for Security and Privacy of Social Networking Sites on Users Perspective

Balogun Abiodun Kamoru
Dept.of Software Engr and Information Systems
Faculty of Comp8uter Science and Information Technology
Universiti Putra Malaysia
Serdang 43300 Selangor Malaysia

Azmi Bin Jaafar
Dept.of Software Engr and Information Systems
Faculty of Computer Science and Information Technology
Universiti P
utra Malaysia
Serdang 43300 Selangor Malaysia

Masrah Azrifah Azmi Murad
Dept.of Software Engr and Information Systems
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
Serdang 43300 Selangor Malaysia

Marzanah A. Jabar
Dept.of Software Engr and Information Systems
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
Serdang 43300 Selangor Malaysia

ABSTRACT

In the digital age, the phenomenon of being able to connect with other individuals has reached some of the most web-traffic (Tuunainen, et. al., 2009).There are risks associated to the SNS which gives the capability to have victims studied in multiple ways to measure and limitation (Chena & Sharma, 2013). There are many different ways a user can prohibit or limit the amount of risk for the SNS, which are: (a) ensuring that the computer and SNS have proper measures in place, (b) nor clicking links, (v) when their profile becomes obsolete ask that the profile becomes deleted, (d) being careful as to what application they use, (e) creating different passwords, (f) being careful on the SNS to ensure that they are limiting the actions that they are doing, and (g) configure and review the SNS privacy policy (2016). There are many studies that prove that the more that someone uses a site that the more they are likely to be victimized (Kirwan, et. al., 2018).. risk measurement models.

General Terms

Social Networking Sites, Risk, Privacy, Security

Keywords

SNS, social networking sites, risk, privacy, security

1. INTRODUCTION

According to various countries laws and BBB, social Networking Sites (SNS) should value the privacy and security of their users and prevent any undesired third-parties and other users from viewing a user’s profile as well as private information (Chena & Sharma, 2013). Users use the SNS platform to share personalized information between selected individuals, family or friends, and intended organizations that they are interested (Tuunainen, Pitkanen, & Hovi, 2009). The users share their private information regarding interests, hobbies, and intimate details about their personalized lives to develop intimate and connect on a personal level with the other users (Narayanaswamy & McGrath, 2014).

SNS are known to have privacy and security risks (Chena & Sharma, 2013). The primary risk comes from when people post information that can be used to find them to people that in real life they do not know or do not trust (Tuunainen, et. al., 2009). The members of the SNS are at risk for malware, spam and phishing, data theft, and content alternation. The members may experience emotional pain, loss in funding, or character damage. A lot of personal information is released during the sign-up process to when the individual posts about their interests (Narayanaswamy & McGrath, 2014).

In response to the SNS privacy and security problems, this study will investigate who the target for the victimization is, possible materials required to commit the crime, and ways to avoid the risks. This report will investigate the various many policies, laws, and theories regarding the cause and the prevention of the privacy and security risks from potential victimization of cyber-criminals. This study will review how popular SNS use the policies as well as their security to review whether or not they are effective.

2. RELATED WORK

In this section, this report will review the risks on SNS privacy and security.

2.1 Background

SNS is various platforms which operate to share confidential data to transmit it between individual users and users to organizations (Tuunainen, Pitkanen, & Hovi, 2009). These users share what they are passionate about and intimate life activities to be linked between their personal contacts (Narayanaswamy & McGrath, 2014). The data has the purpose of bridging users and organizations together for developing substantial connections (Tuunainen, et. al., 2009).
In a few studies, they found that using SNS was made for the purpose of connecting with other individuals (Tuunainen, et. al., 2009). In the example of Facebook, users from the social network create a connection to other users submitting a “Friend” request. This process permits other users to access

the individual's profile information and linking their social networks.

SNS have become a international successful digital age phenomenon (Narayanaswamy & McGrath, 2014). SNS are extremely popular and has been some SNS have ranked in the top end for web traffic (Tuunainen, et. al., 2009). According to www.quantcast.com in 2008, Myspace was ranked the top ten in web traffic with over 47 million United States monthly visitors. In February 2009, Facebook had more than 175 million users.

2.2 Privacy Risks and Security Risks

SNS are known to have privacy and security risks (Chena & Sharma, 2013). The primary risk comes from when people post information that can be used to find them to people that in real life they do not know or do not trust (Tuunainen, et. al., 2009). The members of the SNS are at risk for malware, spam and phishing, data theft, and content alternation. The members may experience emotional pain, loss in funding, or character damage. A lot of personal information is released during the sign-up process to when the individual posts about their interests (Narayanaswamy & McGrath, 2014).

Malware is the device that a cybercriminal uses to obtain user information and login credentials for fraud (Kirwan, Fullwood, & Rooney, 2018). Malware techniques can include clickbait which is either a text or a video, advertising a desirable product or service that is either unattainable or does not exists, and hoax competitions or giveaways. One in third of the 295 Malaysian undergraduate students studied had fallen victim to a SNS scam.

There is several spams and personal confidentiality that are in permanent concerns in SNS (Chena & Sharma, 2013). The information gets traded to advertising and Internet tracking companies. Educational institutes and employers have misused the information available on the SNS (Narayanaswamy & McGrath, 2014). The companies view the photographs from a friend's social networking page and view them as a personal signature to develop an phishing message. The SNS can have legal issues resulting from any information being transferred to unintended parties. The privacy information that gets released may cause stalking, extortion or other dilemmas (Chena & Sharma, 2013).

2.3 Proposed Methods to Prevent Risks

A user can use their own precautions to reduce any possible harm from using a SNS (2016). The first one is to ensure that the computer has proper security measures in place. The second step is to avoid clicking on links. The following step is to request account to be deleted. The fourth step is to type the SNS directly into your browser. The user should be careful about installing any applications. Different passwords should be assigned to different things. While using the SNS, the user should be cautious in all actions that they do. Configure and review the SNS's privacy policy.

The first protection regarding protection comes from the computer as well as the SNS (2016). A good antivirus software, anti-spy software and firewall helps protect against any applications that is not desired on your computer. The computer should be patched and up-to-date. The SNS should also have proper security measures in place.

A good SNS has vendor trust from their clients (Chena & Sharma, 2013). These SNS have made an attempt at constantly improving their platform with the latest security protection. The SNS lower risk perceptions because they reduce Internet risk and value privacy. A proper SNS may have such high security protection that they have been rewarded by the seal of approval by WebTrust, TRUSTe, and BBBOnline. The seal means that the SNS has been known for meeting the privacy requirements by policies and privacy systems, and site designs.

Use caution when clicking on anything (2016). If a link seems suspicious or too good to be true, do not click on it. If it was sent by your closest friends page, then their account may already be hacked or hijacked and now spreading malware. Be sure to contact your friend or family about anything that they are sending you.

If a person feels that their personal information has been put at risk, they may feel that they should not continue to use the server (Chena & Sharma, 2013). If this occurs, request the administration of the SNS to have your account deleted but first remove all of your personalized data. The account should be deleted and not deactivated (2016).

While trying to access the SNS, directly type the address into your browser or use the personal bookmarks (2016). If you click a link to go to the SNS through an email or other website, you may be entering your information into a fake site. This reduces the chances of personal information of being stolen.

Some SNS allow the capability to add and install games (2016). The user should be cautious when installing any applications. There is limited to no quality control and review of applications. These applications may obtain full access to the user's account and information that they share. Malevolent applications may use the access to interact with friends on your behalf as well as steal and misuse personal information. Limit the user's applications choices to trusted and well-known sites and applications. If the user is ceasing application usage, uninstall the application. Some applications may change the user's security and privacy settings.

Passwords should be strong and unique (2016). The vulnerability of accounts increases when a password is the same on all accounts, if one becomes compromised. Assign various passwords for the multitude of accounts being used. The organization that someone works at should not have the same password as a personal SNS account.

A user should be cautious of how they use the SNS (2016). Having too many friends, groups, or pages that the user has joined increases the population that have access to your personal information. Secrets should not be shared, as the privacy on a SNS should not be assumed. The information that should be shared should only be what a individual feels that a complete stranger should know. Once information is on the internet, it stays there for all to be seen and cannot be retracted. Vacations and extended stays should not be announced on SNS. Pictures should have meta data deleted, which is the date and time that the picture was taken.

SNS are willing to work with the people who want to learn how to make themselves more safer (Chena & Sharma, 2013). SNS minimizes the Internet risk perception, increases public awareness, and have educational campaigns. The educational campaigns are supposed to increase end user understanding and abilities in fighting cyber threats and limit the chances of being attacked. They also provide awareness programs to help eliminate the bias that Internet risks as well as a risk assessment.

Configure the privacy settings to attempt to limit other people from using the users SNS account information (2016). Some sites do not automatically limit the people who can view the information. They may permit that other people can post on any users page. By changing the settings, users can hope to limit the people who have access to post and view their account page.

Privacy settings and privacy policy has been something that the SNS has reviewed and the user should as well (2016). A privacy policy was written as a response from privacy risks and threats as such it is regarding only the collection of personal information and the protection laws. The privacy policy may help the user understand what they are giving consent to after they have uploaded personal data into the SNS.

A privacy policy is a notice on a SNS that discusses information regarding the user's personal identifying information by the SNS owner (Tuunainen, et. al., 2009).. It discuss how the personal information is collected, used, whom may know the information, and the security measures taken to protect the personal information. Ir discusses how the law of the country has set out what the legal requirements are to protect the information.

The damage and humiliation that SNS have obtained, if their users private information becomes released to third-party organizations and individuals, has caused them to developed several policies to protect their users (Narayanaswamy & McGrath, 2014). The failure of the SNS policies can be related to three different aspects. The first idea of the unprotection is because of the privacy options have certain biases of protecting only certain users information. It is possible for the users to be unaware of the privacy options available to protect their content. The last option is that the users have not had sufficient knowledge to locate and apply the policy made to protect their content.

2.4 Theories about Victimization

Researchers have studied the reasons why someone would become the victim of cyber-crime. Many users believe that the cyber-crime will not happen to them so the SNS is safe (Tuunainen, et. al., 2009). There are many theories about why it occurs to individuals such as characteristics of the person and Routine Activity Theory (Kirwan, et. al., 2018).

According to Agustina, there is certain details that the victim of cyber crime (Kirwan, et. al., 2018). One type of individual who is likely to become a victim is someone in their late 60s who are well educated but have high levels of depression. Some research has studied the behavior aspects of a victim and found that they have poor decision-making habits. If a individual has tendencies to be high level of agreeableness, impulsive, and extraversion.

According to Burgard and Schlembach, fraud victimization begins when a user experiences a loss of risk awareness and caution is diminished which means that they permit strangers to engage with them (Kirwan, et. al., 2018). They have an unrealistic and self-deceptive actions towards the situation. Password sharing among professions occur when he impulsivity scale finds that there is a lack of perseverance, according to Whitty.

The Routine activity theory, RAT, applies for the cyber-crime (Kirwan, et. al., 2018). This theory states that to have a crime, there needs to be a motivated offender suitable target, and an absence of a capable guardian. The more time that a user spends on a SNS, the increased chance that they will come across a malware and become a suitable target.

2.5 Research Gap

The research that was collected had failed to analyze how effective the policies, laws, and security methods were for preventing the victimization. The cases were used to explain why it occurred instead truly understanding all aspects of the prevention

3. METHODOLOGY USED

What are some levels or determining factors of the victimization of cyber crime due to privacy and security protocols? How can we prevent the victimization due to the risks associated?.

3.1 Design of the Models

This experiment will be based on a qualitative method to understand the reasoning behind the lack of security and privacy. It will evaluate the determining factors as the reasons why other people were victimized. It will co-relate to the risks associated in the research as to the reasoning. The research will be completed by archival research by the same articles as were used for the related works. The research provided allows the research to co-relate exactly to what was theorized in these articles. Due to the date that the other articles were created, it has a limitation of being almost a year outdated.

3.2 Experiment

Myspace saw a trumous loss in population of users after giving away their customer's information (Chena & Sharma, 2013). It occurred after the users found that Myspace was giving their personal information to illicit third-party sources. The user must feel comfortable that the SNS will not share their personal information; however, they are still putting themselves at risk.

Data information had been hijacked Facebook security (Chichioco, et al., 2018).In 2012, there was a scam to try to steal financial information from Facebook users. The message was that their account was about to be disabled and to click a link to verify their account. The users proceeded to follow the Facebook page about their login credentials and credit card information for securing their account.

According to Gross and Acquisti in their 2005 study, Facebook is criticized for the fact that user's profiles are visible to as much audience as possible on the control settings (Tuunainen, et. al., 2009). If users do not change their Facebook privacy settings, the information is available for everyone on the same SNS service. There are very limited amount of individuals who will change their privacy settings for the user's profile. According to Cranor et al in their 2006 article, despite great efforts of the SNS to create interfaces and features, most users rarely change their account settings to any of their SNS.

According to Govani and Pashley in 2005, when users of Facebook were being studied they had an awareness of the privacy concerns and how the privacy protection was available through Facebook (Tuunainen, et. al., 2009).. Users understand the consequences that may occur due to providing personal identifiable information to the population. The users felt comfortable enough with giving their personal information. The users knew that there were ways of reducing the chances of someone they didn't want to view their profiles, but they were indifferent about them seeing it. The users did not take any precautions to protect their information. According to Tow and all in 2008, users had either been unaware of the issues or they felt the risk was very low. The users had a naive sense that online communications are safe.

The results of the victimization study has shown more experience with the SNS have a increased chance of falling victim to the scams (Kirwan, et. al., 2018). RAT predictions are positively correlated as an increase of presence through the SNS in time results in higher victimization risk. There connections between impulsivity and victimization were weaker than expected. There is an openness to experience and susceptibility to scams. Certain types of malware may cause the cybercrime phenomenon although it is unclear which ones.

3.3 Data Collection

There are certain variables that make a user more likely to become a victim of cyber crime from privacy and security. The SNS knowingly giving away information to third parties, such as Myspace (Chena & Sharma, 2013) and Facebook (Tuunainen, et. al., 2009). Facebook had been previously hacked to victimize their users in providing credit card information (Chichioco, et al., 2018). Users should know that they could be a victim of cyber crime if they use it a lot (Kirwan, et. al., 2018) or use Facebook (Tuunainen, et. al., 2009).

There are ways to prevent victimization because of the risks. Myspace users should have their accounts deleted and personally delete all of their information (Chena & Sharma, 2013). Facebook users should type Facebook into their web address and change their privacy protection. There should be training on protecting the user if they use it SNS a lot (Kirwan, et. al., 2018) or use Facebook (Tuunainen, et. al., 2009)..

4. DISCUSSION

There are risks associated to the SNS which means that there has been a measure and limitation for becoming a victim in many studies (Chena & Sharma, 2013). There are many different ways to protect themselves, which are: (a) ensuring that the computer and SNS have proper measures in place, (b) nor clicking links, (v) when their profile becomes obsolete ask that the profile becomes deleted, (d) being careful as to what application they use, (e) creating different passwords, (f) being careful on the SNS to ensure that they are limiting the actions that they are doing, and (g) configure and review the SNS privacy policy (2016). There are many studies that prove that the more that someone uses a site that the more they are likely to be victimized (Kirwan, et. al., 2018)..

Many individual users are putting themself at risk. In the digital age, the phenomenon of being able to create lasting bonds through the internet expanded into one of the top web-traffic (Tuunainen, et. al., 2009). They are at risk for malware, spam, identity theft, and people altering their profiles. Users should try to use the SNS that have an approved seal (Chena & Sharma, 2013). Many people feel that the SNS is safe and have an idea that it won’t happen to them (Tuunainen, et. al., 2009)..

There are more studies that need to be completed (Kirwan, et. al., 2018). Some more research needs to prove what is the malware that is used for the individuals that are currently using SNS a lot. They need to review how does the legal aspect of cyber-victimizes occur in SNS (Tuunainen, et. al., 2009).

4.1 Future Work

There are two proposed studies that should be completed. There should be a quantitative study to test how many individuals have followed the method to safely secure themselves. There should be a combination of quantitative and qualitative study to test how effective the privacy and security trainings are as well as how many people attend them.

5. CONCLUSION

SNS have risks which has been studied in many articles. They found that the more someone uses the SNS the more they are likely to be a victim of a cybercrime (Kirwan, et. al., 2018).

6. ACKNOWLEDGMENTS

Our thanks to my Research advisor in person of Associate Professor Azmi Jaafar, Associate professor Marzanah A Jabar, Associate Professor Masrah Azrifah Azmi Murad and to my Colleague Umar B. Majid and lastly to Research Grant VOT Feb/2020/UPM

7. REFERENCES

[1] Chena, R., & Sharma, S. K. (2013). Understanding Member Use of Social Networking Sitesfrom a Risk Perspective. Procedia Technology,9, 331339. DOI:10.1016/j.protcy.2013.12.037.

[2] Chichioco, A., Doshi, C., Qualman, E., Redka, M., Attard, D., Bhattacharya, J., . . . SocialnomicTrends. (2018, February 22). 4 Case Studies in Fraud: Social Media and Identity Theft. Retrieved April 23, 2019, from https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-thft/

[3] Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk Factors for Social Networking SiteScam Victimization Among Malaysian Students. Cyberpsychology, Behavior, and Social Networking,21(2), 123-128. DOI:10.1089/cyber.2016.0714

[4] Narayanaswamy, R., & McGrath, L. (january 1, 2014). A Holistic Study of Privacy in Social Networking Sites. Academy of Information and Management Science Journal,71-85.Retrieved April 23, 2019, from https://www.questia.com/library/journal/1G1-397579760/a-holistic-study-of-privacy-in-social-networking-sites.

[5] Social Networking Sites: Security and Privacy Issues. (2016).RetrievedApril23,2019,fromhttps://www.citizensros.com/docs/newsletters/social-Networking-sites-security-and-privay-issues.pdf

[6] Tuunainen, V., Pitkanen, O., & Hovi, M. (2009). Users’ Awareness of Privacy on Online Social Networking sites – Case Facebook. EConference Paper,1-16. Retrieved April 23, 2019, from

[7] https://www.researchgate.net/publication/205694735_Users'_Awareness_of_Privacy_oonlinSocial_Networking_sites_-_Case_Facebook