ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

Securing Social Media: Security Tips and Best Practices

Dr. shashirekha Malagi

Assistant Professor of Law, Sir Siddappa Kambali Law College [Formerly University College of Law], Karnataka University, Dharwad, Karnataka.580001.

ABSTRACT: The Internet is a treasure trove. It provides an excellent communication platform through countless applications such as online forums, online chatting channels, video streaming, blogs and many more. All these are termed as Social Media .Considered to be the greatest technological innovation ever discovered, Social Media is fast gaining popularity globally among Internet users. They allow people to share ideas and interact with other people, from old friends to strangers. This interaction reveals a lot of information, often including personal information visible to anyone who wants to view it. This article will illustrate and discuss the most prevalent issues and threats targeting different types of social media and Security tips and best practices.

KEY WORDS : Social media, Security Threats, Crimes, Security tips and best practices, Security strategies, Act, Misuse, Supreme Court.

I.INTRODUCTION

Social media is a want of life for everyone, without which no one can live. Every person is present on the web eagerly, and some are prone to unwanted risks and issues. Nowadays, social media plays a dominant role in the society. The resources that are used for accessing social media are computers, Smart phones, and other Internet connected devices. People with all ages possess these devices to interact with the outside world through various networking sites and pages. The main idea behind the social media is the platform that makes users to express their views and concerns regarding anything and sharing it with other people on the same platform. These also includes posting of photographs, videos, activities etc. They can reach any people near or farther away from their place. Despite providing all these advantages to individuals it is essential to observe the shared information is not as secured as one believes. Certain users try to gain profit by exploiting another person's information. These acts include cyber bullying, harassment or cyber-stalking. These attacks are common threats to teenagers who continuously spend their time on social media with intent of becoming popular. They are often carried away by rumors spread by someone on the same platform. Hacking individual's account to post something illegal or inappropriate description of one is the common act in social media. This act during extreme situations has also forced victims to commit suicide. Therefore, every individual before posting any information regarding oneself should be aware of the consequences.

II.SOCIAL MEDIA SECURITY THREATS

When you first think of social media threats, what most people might point out are trolls, fake accounts and fake followers via purchased services, or maybe the "fake news" accusations flying about everywhere. What's often overlooked in social media security, though, is how it can be used to harm organizations and their customers via threats such as brand impersonation, fake corporate accounts, and phishing or ID theft scams that are all run via social media platforms.[i]

Examples of Social Media Security Threats

a. Posting links on Twitter on Facebook to direct people to websites that will download malware

b. Using fake accounts to post fake promotions or discounts that set customers up for phishing scams

c. Impersonating corporate CEOs to secure personal data from customers believing they're speaking with an executive

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

d. Communicate false information in order to manipulate a company's stock price

e. Build an unauthorized brand-related profile in order to sell it to the organization that wants control over their legitimate content.

III. CRIMES IN SOCIAL MEDIA

The practice of various social media applications such as WhatsApp, Facebook and Twitter has gained much popularity in recent times altering the means of understanding and facing e-crimes and victimization. Formerly, people had an idea of social media crime based on the posts that were posted. In fact, the Social media has also designed new apprehensions associated with crime itself.The abuse encountered in social media platforms are not unusual. With increasing developments in digital technology, social media has gained every positive and negative aspects related to criminal justice and law. Therefore, Social media has initiated new prospects in solving crimes by the criminal justice agencies.
Some of the most frequent crimes committed on, or because of social media are:[ii]
a. Online Threats, Stalking, Cyber bullying: The social media crimes includes threats, bullying, harassing, and stalking individuals online. Since most of the activities goes unaddressed or without charging of any penalty, victims of the crimes often be ignorant about reporting it to the officials.[iii]
b. *Hacking and Fraud*: Hacking refers to the process of illegally logging into another user account to perform ill-legitimate activities like embarrassing the users through awkward posts, generating counterfeit accounts, or impersonation accounts. The main purpose of hacking and fraud is to trick users and gain any kind of benefits showing that they operate from a legitimate identity.[iv]

c. Buying Illegal Things: The process of buying illegal things such as drugs, smuggled products, gold etc are punishable by law. These activities are now increasingly carried out through online social media.[v]

d. Posting Videos of Criminal Activity: The increasing usage of smart phone and digital technologies, most of the convicts post criminal video activities on social media. This creates shock among various users watching them but at the same time are useful for police divisions and lawyers to seize and imprison the offenders.[vi]

e. Vacation Robberies: Most of the users have a habit of posting all their daily personal activities on social media. Hence, burglars follow these types of users through their social media account and identify their vacation occasions to gain any monetary benefit.[vii]

IV. COMMON SOCIAL MEDIA SECURITY RISKS

Users who leave their social media accounts unattended for long period of time have more chances of being victims to attackers. Hackers collect all unattended reports of user accounts and choose one or some to post illegal or fraudulent messages in actual user name. Users who are present in the same platform consider these actions are carried out by the actual user. By this way, other users may also become victims to the attackers when they click or open any link posted from that account. The individual will be unaware of these activities until they are notified by customer help supporters.[viii]

Some of the social media security risks that occur common can be listed as follows,
Human error: This type of risk is very common. There are no perfect individuals each of them may commit mistakes unknowingly. Carelessness might lead to even large threats within the organization. Any inappropriate action may include simply downloading a dummy file that contains virus or any other threats. A recent survey has proved that the major cause of cyber threats in an organization is due to the carelessness of the staff members.[ix]
Third-party apps: This type of risk happens when an individual purchases applications or services from third-party service providers. These apps are prone to vulnerabilities caused by attackers due to poor security measures. When user installs a third-party application then the work of a hacker becomes easy by intruding into the system through the security loopholes.[x]
Phishing attacks and scams: Phishing attacks are very common. A fake email is sent in the name of a trusted user to perform actions such as clicking or downloading of a link or attachment. By this the attacker gains access to

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

confidential data asking user to provide with details such as passwords, account numbers etc.,These scams also redirect users to inappropriate Webpage posing them to several risks.[xi]

Imposter accounts : Imposter accounts are those that appear as trusted accounts for other users. The increase in the fraudulent accounts have raised over years. Attackers create these accounts unofficially to gain profit in some way or other by fake messages or calls. They request for user's confidential information in an official manner and exploit them even without the knowledge of the user.[xii]

Malware attacks and hacks: At present, the hackers in social media have evolved world-wide. Hackers use a counterfeit profile to associate with workers of besieged administrations. By allocating a file with the invaders, they gain inaccessible entree to the target computer systems.[xiii]

Privacy settings: Every individual experience both advantages and disadvantages of using social media to post privacy contents. Most of the users know that their data is not as protected as they think. The level of privacy in social media is considerably very poor. Despite knowing all these issues people still choose to use their own social sites of their interest. This privacy issue is generally a higher form of risk for organizational users where accessing social media is done for personal or business purposes.[xiv]

Unsecured mobile phones: a user can simply log on to any social network with a single click. If these devices are lost or being stolen without any proper security methods employed, it will result in undertaking of social accounts by the attacker. They easily gain access to the accounts on the devices with a single tap. They also perform phishing or malware attacks to other contacts on the devices. Hence, proper authentication mechanisms should be provided on individual's mobile phone for preventing from serious attacks.[xv]

V. SOCIAL MEDIA SECURITY TIPS AND BEST PRACTICES

Securing social media can be done only if the organizations continuously monitor for any new threats across the social networks. By examining continuously, the occurrence or instance of false interpretation of their organization then they are immediately reported and eradicated. With the help of this reporting process, the customers can be given an alert message through their official account in case of any serious threat issue identified.[xvi]

One major attempt that helps to clear threat issuess by limiting publishing rights for users present in the social media channels. There should be distinguished rights between the user and the admin credentials. Every staff member should not be given access privileges to manage the account. A regular process of remedial connection is to be done in order to maintain a robust defense social media security strategy. A large interconnection of people may lead to large risk exposures. Hence social media security is a must in mitigating the risks that cause severe damages to the organization as well as to an individual.[xvii]

Some of the social media security tips and best practices are:

Generate a social media strategy: Every corporate organizations and employees are equally responsible in maintaining the security of their social media sites. For this purpose, they are assisted with various policies that protect them from various threat issues. These policies also help them from legal troubles and financial loss. Some of the social media policies that are assisted along with organization can be as follows:[xviii]

a. Explaining the company's brand on the social site with the help of some guidelines
b. Ensuring the confidentiality of the personal use in the social media with the help of rules
c. Identifying the social media account for responsible in charge of departments and the team members
d. Confidentiality and copyright attested guidelines
e. Rules for creating strong effective passwords and mandatory password change periodilly
f. Updating the software and services consistently
g. Systems to identify and prevent security threats such as scams, phishing mails etc.,
h. Generating notifications and responding to any new security concern identified.

Training individuals on social media security best practices: A major cause of cyber threat in social media arise due to the carelessness of the staff members. Hence the staff members are to be provided with proper educational practices on how to prevent themselves from being a cause to an attack. Even if organizations are provided with best security policies, they can be easily violated if employees do not pay attention to them.The training sessions help them with

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

enough knowledge to pose questions in case of new security issue encountered. They are also provided with awareness training on current threat issues. Apart from educating the staff members suitable training tools are also equipped that helps them in overcoming the security issues.[xix]

Limit social media access: The threats to an organization's social media not only come from the outside world but also caused by the employees present inside them. The chances of employee exploitation are greater than a hacker exploit. This issue can be defeated by limiting access to the social accounts. An organization may have large number of people or teams managing the account in many forms such as messaging, post creation, or customer service. Hence, the admin is responsible to set access privileges by limiting users to post or make any modifications for security purposes. The admin provides Hoot suite software for enabling right access to authorized employees. This is based on the idea admin creates account and no individual is prescribed with separate login information. When that individual resigns from the company then that particular account will be terminated without having burden to change passwords provided on the social network.[xx]

Set up a system of approvals for social posts: The owner of the organization is responsible to set up approvals for all the employees who are accessing the common social media account. By these approving methods, the users who can only the right access can post or make changes to that particular organization's account. Hoot suite is a tool that gives workforces or outworkers the capability to draft posts and post them with a single press. But the final approval is given only by the reliable individual on the lineup.[xxi]

Put someone in charge : Appointing a responsible individual as in charge of monitoring the social risks helps in minimizing the threats and issues. The responsibilities of this key person involve determining the users containing publish access rights, monitoring the presence of brand on the social site and the policies owned for security maintenance purposes. This person will be mostly the one who holds seniority in the marketing team maintaining a healthy relationship with company's IT department and play an important role in an organization's social media security development. This person also scans for members who might make mistake posing organization into risk that may vary from security issues to damaged reputations.[xxii]

Keep track of accounts and involve in social listening: As stated earlier, social accounts that are unattended for long period of time become ripe for hacking. By continuous monitoring of social channels ranging from daily usage to subscribed but unused cases. Designating a person to keep track of the legitimate post on the accounts. Cross-referencing the posts against one's content calendar may be considered as primary step. Following on anything unexpected is necessary. Despite having the appearance of legitimate post, can contain serious issues too. It usually may be unsophisticated human error or large access gaining of individual's account. It is also important to watch for imposter accounts, any unwanted conversations about company's brand and untimely indications of organization's product by workers (or any allied person).[xxiii]

Invest in security technology : Even though the social channels are monitored by users that cannot be done all day long, software helps in those purposes. ZeroFOX are security software technology which automatically alerts of security risks. Hoot suite dashboard complemented with user integration of ZeroFOX helps in providing the following alerts :

a. Notifies malevolent links displayed on social media.
b. Alerts users of hazardous, hostile, or invasive contents aiming organization's product.
c. Blocks scams that points the organizations and employees.
d. Identifies fake accounts imitating the product.
e. Provides protection against hacking and phishing outbreaks.

Accomplish a regular audit: The evolution of social media has also paved way for many social media security threats that are inconsistent over time. This is because the attacker finds new technologies and implements them thereby affecting the individual or organization's social systems in the form of malwares or scams. Hence social media security measures are in the necessity to organize regular audits to stay ahead of the bad actors.[xxiv]

Social Media Security strategies: The social media security procedures emphases on providing a non-conceded security to the users. While designing these procedures, user must recognize the security area of concerns, ways to attain security, and persons in-charge of providing them. The procedure must also include an area that ranges from usage of social media applications to the user private terminals such as mobile devices, network security, and firewall boundaries. The private network computer security is sustained by IT sector, responsible for granting or denying the capability to access features, possessions, and execute several activities. Since Public social media sites are outside to the organization's network, the control possibility are not extended to those locations.[xxv]

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

Some of the general tips :[xxvi]

a. Protect your password.

b. Use Facebook's extra security features.

c. Make sure your email account(s) are secure.

d. Logout of Facebook when you have finished your work.

e. Run anti-virus software on your computer.

f. Think before you click or download anything.

g. Never give your username and password out to untrusted third parties

h. Sign out of your account after you use a publicly shared computer.

i. Manage your account information and privacy settings from the Profile and Account sections of your Privacy & Settings page.

VI. ACT ON SOCIAL MEDIA MISUSE: SUPREME COURT

`The Supreme Court recently expressed the need to regulate social media to curb fake news, defamation and trolling etc., by enacting Act on social media. It also asked the Union government to come up with guidelines to prevent misuse of social media while protecting users' privacy. The apex court made these statements while hearing a transfer petition by Facebook which has asked for petitions on regulation of social media filed in Madras, Bombay and Madhya Pradesh High Courts on similar issues to be transferred to the Supreme Court so that the scope can be expanded.[xxvii]

A bench of justices Deepak Gupta and Aniruddha Bose expressed serious concern over some social media platforms not being able to trace the originator of a message or an online content and said the government must step in now. The bench also said neither the apex court nor the high court is competent to decide this scientific issue and it is for the government to come up with appropriate guidelines to deal with these issues. Expressing concern about intermediaries like Facebook and WhatsApp not being able to trace the originator of an offending post or content, the top court said it is a "very serious issue" as it also involves terrorism, pornography, paedophilia, fake news and trolling.

The court stressed that guidelines must be framed keeping in mind the privacy of individuals. At the same time, they must help in maintaining the sovereignty of the country.The bench of justices Deepak Gupta and Aniruddha Bose sought to know what kind of statutory regime could be put in place to prevent the spread of fake news and hate, terror and porn messages through social media. Solicitor General Tushar Mehta said the government has framed draft rules and suggesions.[xxviii]During the hearing, Justice Gupta said, "I don't think the Supreme Court and high courts should decide how intermediaries should work." But the "misuse of social media has become dangerous. The government should step in at the earliest to deal with the situation. We can't say we don't have the technology to trace the origin of online crimes. If the originator has the technology, we have the technology to counter it."[xxix]

VII.CONCLUSION

To secure the social media from various risks, popular security tips and best practices are provided to users to prevent themselves from being victims to social media crimes. Social media security discusses to the process of securing the powerful social media content from threats or issues that may be caused due to the attackers. Every organization at some point of time becomes victim to these issues that may result in any major or minor loss both to the organization or to the individuals present in it. Maintaining social media security for large enterprise networks is often defined as a critical process ,since it involves numerous factors. Some of the measures to ensure security are preventing fraudulent use from scams phishing attacks or account compromise, protecting corporate accounts, and defending against various other attacks. Operating any of the social media channels without following preventive measures may

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

put you into serious jeopardy. It will create harm to your personal or company image in the long term. The dangers can be avoided by following the simple steps mentioned above and stay alert from hackers and fake account users.

REFERENCES

[i] https://fraudwatchinternational.com/social-media/social-media-security-best-practices/, (visited on 12.12.2019)

[ii] http://eprints.lse.ac.uk/65465/1/blogs.lse.ac.uk-How%20social%20media%20is%20changing%20the%20way%20people%20commit%20crimes%20and%20police%20fight%20them.pdf, (Visited on 2/12/2019)
[iii] *Ibid.*
[iv] *Ibid.*
[v] *Ibid.*
[vi] *Ibid.*
[vii] *Ibid.*
[viii] https://www.rswebsols.com/tutorials/internet/privacy-security-risks-social-media,(10.12.2019)
[ix] *Ibid.*
[x] *Ibid.*
[xi] *Ibid.*
[xii] *Ibid.*
[xiii] *Ibid.*
[xiv] *Ibid.*
[xv] *Ibid.*
[xvi] https://thesai.org/Downloads/Volume7No2/Paper_2-Role_of_Security_in_Social_Networking.pdf,(Visited on 3.12.19)
[xvii] https://blog.hootsuite.com/social-media-security-for-business/,(Visited on 12.12.2019)
[xviii] https://fraudwatchinternational.com/social-media/social-media-security-best-practices/,(Visited on 3.12.19)
[xix] *Ibid.*
[xx] *Ibid.*
[xxi] *Ibid.*
[xxii] *Ibid.*
[xxiii] *Ibid.*
[xxiv] *Ibid.*
[xxv] *Ibid.*
[xxvi] https://www.qcert.org/sites/default/files/public/documents/cscsps_guidelines_for_securing_social_media_accounts_eng_v2.1.pdf,(Visited on 20.12.20190
[xxvii] https://www.deccanherald.com/national/act-on-social-media-misuse-supreme-court-to-centre-763758.html,(Visited on 3.12.19)
[xxviii] *Ibid.*
[xxix] Read more at: https://www.deccanherald.com/national/act-on-social-media-misuse-supreme-court-to-centre-763758.html,(visited on 4.12.19)