Social networking security

Business

Abstract Social networks have become a part of life of most people. Their global popularity is rising by the day. These networks provide a form of interaction service to its subscribers. Examples of these social networks areFacebook, MySpace, LinkIn andTwitter.

Popularity of social networks began in the early 2000 and rose significantly over the last decade. The pioneer of these was MySpace network which saw better times between 2000 and 2004 when Facebook was launched. Facebook outgrew MySpace network and has since taken over as the most developed and famous social network globally. By 2009, Facebook had a staggering 900 million followers globally. These networks are web based databases that provide an interface through which people can interact.

This interaction is always through sharing of photos, thoughts, emails and ideas on the internet. Unlike their earlier versions, modern social networks are so complex in nature that offers a wide range of services. It’s, therefore, no surprise that most corporate bodies and businesses have a keen interest in using them to reach as many customers and large markets as possible. Equally, their benefits to humanity as a whole are undisputed. People have taken to these social networks with a dedication never seen before.

Everyone attaches a great deal of importance to these networks to point that not a day goes by without a peek into either Facebook or Twitter. Unfortunately, social networks have not been spared the fate of most other web based applications. They come with a fair share of security concerns and issues that pose both personal and organizational threat. Although, these threats are real, they don’t offer a good enough basis for scrapping off social media as a whole. Instead, users and producers of these networks should devise means of limiting these threats in order to enjoy the benefits they provide. This paper seeks to provide an analysis of common security issues associated with social network and how best to mitigate them.

It also shades light on special security features and applications like encryption and decryption standards and their benefits. Thesis statement Security and social issues associated with social networks should not be taken as an excuse to discard the use of such networks either for business or personal benefits. Instead, they should be viewed as opportunities to achieving the promises of technology. Introduction The benefits of social networks opposed to their potential harm are the subject to debate on. However, one fact stands out: used prudently, social networks have huge returns on investments especially in the business perspective.

That’s why there exists an urgent need to keep their use within a safe limit both from the business and personal perspectives. From the business point of view, social networks can secure enviable comparative advantage by using the social network as a marketing strategy. This way, a business stands a chance of reaching many customers at the least possible cost, since social networks like Facebook are cheaper than advertisement (Financial Times Lexicon 5-9). This will ultimately lead to an increase in sales revenues. At the same time, careless use has a potential to cause immense damages and losses. Such losses usually result from leakage of confidential data that may give an edge to the business’ competitors or can be losses occasioned by malware.

The base line here is that businesses need to set up clear security policies to cushion themselves from the security threats posed by social networks. These common security issues are as discussed below. Analysis of Most Common Security Issues in Social Media Social network’s popularity has come with both blessings and curse alike. The blessing is seen in the sense that these networks provide an interface through which people can interact freely. This interaction can be revealed through sharing of ideas, thoughts and personal life.

In fact, many married couples made through the social media. As to businesses, social media has provided them with a very effective yet cheaper tool of marketing when compared to mainstream marketing tools like advertisement. In a nutshell, the benefits of social media are as many as the various ideas that are exchanged daily through these networks. Unfortunately, utter carelessness by many subscribers in divulging information has converted social networks into a large vault of delicate information with little concern to keep it private. Although this has attracted the least desirable guests whose main aim is to use such sensitive information for personal endeavors, it’s hardly reason enough to apply non selective measures such as total ban of social network use.

Protecting personal information lies with individuals. Therefore, people should exercise outmost discretion in letting out such information which usually compromises their safety and happiness at a later stage. It’s important to note that cyber criminals have limits too in their line of work. They would almost cease to exist if every person in the social network paid due attention to the amount of information they put online. Until this happens, we should contend with the likely company of cyber criminals who can only do so much harm depending on how much facilitation we offer them. Common security issues associated with social networks are quite manageable.

In fact the best yet cheapest form of managing these security issues is as simple as keeping private information private! Once this is done across the subscriber base, the network providers can then join in by installing better antispyware and antivirus to the systems. At least then they would be almost certain of the origin of any cyber attacks. Before this is done, social network users will have to make do with security solutions that are currently available in the market to combat known security and privacy issues. These security issues are discussed more in the next section under the vulnerabilities and attacks on social media. Vulnerabilities and Attacks Social Media Faces As stated above, social networks have and continue to attract massive following.

Whereas it’s these numbers that make social networks an ideal tool for both business and personal gains, the same numbers have attracted hackers, whose sole aim is to manipulate the system and gain access to vital information of unsuspecting followers. This brings many security issues associated with the social networks. The common security issues associated with social networks that have a direct harm to business corporations are as discussed below: Malware This refers to malicious software that are developed and used by attackers to gain unauthorized access to a victim’s computer. The aim of this access is usually to acquire confidential information. Malware incorporates a number of unwanted software including Trojans, viruses, worms, spyware and Zombies (Malware Revolution 20).

Malware have varied manifestations which makes it cumbersome to control. The fact that they are programmed just like genuine software allows them a wide infection scope with minimal detection even if security applications like firewalls are installed on the victim’s computer. A survey of leading business corporations in 2009 showed that at least 70% of the respondent’s maintained an active presence in the social network. These companies were positioning themselves to enjoy the benefits of marketing through the social networks. However, a survey contacted later in the same year showed a stark contrast to this phenomenon.

54% of these respondents had banned the use of social media while at work and about 20% still condoned its use for business (Gaudin 32). The explanation for this transformation was the active threats arising from Malware attacks witnessed in the social networks. Corporations were contending that the threats arising from social network use were untenable despite the accruing benefits. Inadvertent Disclosure of Sensitive Information The other security issue facing corporation as a result of social network use is the disclosure of information by the company’s employees on social platforms like Facebook and Twitter. Companies have alluded that the increasing use of social networks by its employees threatens the security of its trade secrets and confidential business practices. These concerns are not groundless.

Studies have shown that most employees have adopted a culture of using the company networks to access social networks like Facebook and Twitter accounts (Schroeder 34). Ideally, this culture would be harmless if such employees observe safe use of the services without divulging too much information to the so called ‘ long term online acquaintance’. The general weakness by most workers is the tendency to be too free with such online relations to a point of dropping their guard and posting some rather sensitive data about the company. Consequently, the company ends up losing its trade secrets to their competitors (Waxer 29). For this reason, many companies have been forced to reduce the use of social networks by employees while at work.

In some instances, they have set in place restrictive online security policy that regulates the use of social networks both at work and off work by their employees. Currently, many companies have steered off the use of social networks for security concerns. The biggest concern of these companies is the inadvertent disclosure of sensitive and confidential information. This can happen either as result of deliberate attempts by corrupt employees to gain unauthorized access to such data or as a result of genuine mistakes (Waxer 31). Location Disclosure and Cyber Stalking Social networks like Facebook and MySpace provide an interface through which friends can interact and share practically anything with their online friends. Whereas there can be nothing wrong with sharing photos and ideas on such networks, some information needs to stay private and only known to trusted friends.

Unfortunately, followers of such networks do not set a limit in posting this information. Facebook followers are the notorious lot with some posting crucial data such about their exact location, profession and family members. They even go an extra step of disclosing their contacts online and what schedules they have for the summer holiday. Such information may look and sound normal but the growing online security concerns need to be taken as an excuse of privatizing this information. Privacy would be the obvious reason not to post your location and contacts. Posting such information online makes it easy for criminals to track you down and either rob or harm you for that matter.

Additionally, there are special professions that are sensitive both for personal reasons and national interests. Holders of sensitive jobs like intelligence should not post their location and contacts online. In fact, such individuals should not use their credentials online so as not to compromise their safety. A good example to drive the point home would be the Sir John Sawer’s case, an incoming head of British intelligence-MI6 whose wife posted their home location, family composition and Mr. Sawers’ profession.

This was a big gamble with their family’s safety, given her husband’s job. This information could easily get into the wrong hands of terrorist which could have lead to disastrous consequences (Evans 23). These security issues associated with Facebook are made more complex by the fact that information that one would have wished to remain private ends up being seen by general public. Facebook has been put on spot many times by extending the level of feasibility even to private account profiles. This privacy breach is worsened by faulty privacy agreements that unfairly claim the ownership of all uploads made by the Facebook users (Facebook Privacy Policy).

Insufficient Authentication Control This security issue is faced by business corporations that have large base of workers sharing common devices and passwords in the company’s networks. This makes it a treat especially when minimal or no supervision whatsoever is imposed on them. Security breaches occur when these workers are inexperienced in safe data handling. This usually results in crucial data losses either through deletion or malware activities, since such workers may not concern with updating the antivirus application or devise scanning. The most disastrous threat is sharing administrative password which has links to sensitive data storage of the company.

Inexperienced workers could be duped to open a malicious document which would allow the attacker access to the company’s servers since access to one account means access to all accounts. Phishing The rising use of mobile devices to access social networks has opened up an avenue for hackers to manipulate their victims into surrendering crucial information. The rate at which Phishing attacks is developing is perhaps the highest of all cyber crimes. This phenomenon clearly shows that many people are yet to adopt any security policy during their online interaction. Somehow they easily let off their guard and trust all content that is coming from ‘ an online friend’.

They hardly scrutinize any contents from friends’ emails or correspondence. Two reasons explain this security lapse; one is rather obvious, run away trust! Most social network subscribers get so used to their online friends and gradually learn to trust them. Unknown to them, their friend’s accounts could fall into the hacker’s hands anytime. This means that not everything that comes from them is safe, hence the need to be cautious. The second reason borders on the technical set up of mobile devices like smart phones.

Smart phones do not have the capacity to identify genuine links from fake ones. Consequently, scammers are able to send phishing messages that direct victims to fake login screens with so much ease. Once the innocent victim logs on to these fake sites, there login information is harvested and sent to the attacker's email. This leads to a total takeover of the account (Baker 22). Hackers could then use this information to send messages with juicy subjects to other victims using the hacked account.

These messages always contain links that when clicked would initiate malware activities that harvests up sensitive information. This step is usually successful because the third party victims would not scrutinize the message so much since it comes from someone they know. Cross Site Scripting (XSS) It is a form of attack in which a victim's browser is duped to execute a file with malicious content. Once the file has been run, the attacker can then acquire the victim's credentials and impersonate him to send unsolicited contents to the victim's friends without him knowing. The common acts are sending of obscene contents to the victim's friends. In worst cases, the attacker asks the victim's friends in the name of the victim to send some money as the victim (the account holder) has run into a problem of some sort and urgently needs financial help (Timm 12).

Cross Site Request Forgery (CSRF) This form of attack resembles the cross site scripting in that for both cases; the attacker dupes the victim to execute an unwanted action. The victim is always kept in the dark unless he is crapulous enough to notice any variation. In this attack, the victim is provided with a cookie and asked to click it in order to identify with a given site. An example of an attack scenario is as shown below: Victim logs into a desired website and is provided with a cookie that identifies him and the cookie is stored in the web. The victim goes about his business and logs into another site while still logged on to the current one. Unknown to the victim, the second site may be infected with malware.

This malware siphons the user’s credentials in the first site to execute unwanted tasks which may be to change the user’s password and email it to the attacker’s mail of choice (Burns 24). Information and Data Integrity The biggest security concern by most businesses and individuals today is to protect the integrity of data and information. Security issues with data arise in two forms. One is the intentional tempering of data by attackers by use of malware and the other is the unfortunate instances of genuine mistakes. Social networks are open to many threats and security issues from attackers who use malicious software to alter information in storage or on transit with the aim of sending unintended messages to the business customers. It is mainly motivated by unhealthy market competition where one company may contract the services of a hacker to manipulate its competitor’s information to the public.

Data integrity can be compromised by mistakenly posting the wrong information on the company’s social network wall. The company’s recourse measures to correct the mistake may not fully correct the mistake since the customer’s perception will have changed. This may greatly hamper the company’s business operations. An example of mistakes associated with data handling can be posting out financial results with errors showing that the company has suffered a half year loss. Although the error may be feasible, the investors may impulsively embark selling of their stocks which would greatly reduce the value of the company. Insufficient Ant-Automation CapabilitiesMost malware attacks are designed in varied technologies.

One of the features associated with these malwares is the ability to be automated. This means that once they have been successfully incorporated into a server or a network, the infection spreads automatically throughout the servers of the infected network. This was facilitated by the lack of competent anti-automation applications in most of the social networks like Facebook. In fact this is the main reason that companies, both private and public are contemplating a total ban of social networks in their operations until such time that the social network providers develop these anti automation applications. For example, in 2009, the American army threatened to ban social networks in their operations until anti-automation devices like CAPTCHAS were installed in their network (Schachtman 19).

Law Enforcement Prowling and Network Tapping Maintenance of peace and order is in no doubt a crucial mandate of the government. It’s often argued that the government needs to employ every trick in the book to guarantee everyone’s constitutional right to safety. However, the actions of prowling the social networks by government agents like the FBI may be an infringement on the people’s privacy rights. It is totally acceptable for the Federal Bureau of Investigation to have a social page through which people can volunteer information. What is not right is to have them tap into people’s private profiles and pose as friends yet their main business is snooping around.

If anything, their actions of impersonating friends in order to nab criminals may be a step too far out of their constitutional provisions. The case in which the FBI finally caught Maxi Sopo, a fugitive who had evaded the police and moved to Mexico is laudable. However, the act of impersonating Sopo's friends is a violation of human rights. This shows one of the many instances that government agencies have manipulated the security loopholes in the social networks to further their endeavors with impunity (Lardner 33). Security and social issues that face common users Most of the security and social issues discussed above affect corporations and other social entities.

This does not mean that online social networks have no effects on individual users. Below are examples of issues faced by individuals; Cyber stalking There have been many cases where individual users have been stalked. This has been mostly common with Facebook subscribers where third party agents have used such private information as residence address to tract down victims. The best way to mitigate this is by keeping residential addresses private and not posting it online. Tapping and rogue online friends Many individuals have become victims to fake friends.

This is mostly common with government agents who pose as real friends but whose main intention is to monitor private life with intention of unearthing long lost criminal operatives. Loss of private credentials Just like business corporations, many individuals have lost personal information to hackers through phishing attacks. Recommended Strategies of Addressing the

Privacy and Security Issues Most of the discussed privacy and security issues have a direct link to end user short comings. This means that best way to tackle these security threats should be centered on the end users themselves. This does not in any way disregard the crucial role of other measures like the installation of antivirus.

It only means that mitigation of these security issues becomes easier when end users are well equipped with prevention and recourse actions. The following are the recommendations to deal with the aforementioned security and privacy issues: Observance of Strict Desktop and Password Security Policy Workers should be encouraged to have a password protected screen at all times to prevent any unauthorized access to their computers. More so, these passwords should always be on and timed to go off automatically within a minute of being idle. Otherwise, it would beat the logic to have a password protected screen which locks up after one hour of being idle! Network administrators should also train the workers on how to create strong passwords. Leaving a computer unguarded for even one minute may be all the time that a corrupt workmate need to access confidential data or even install a malware. Equally important, workers who share passwords should be closely supervised and warned against unsafe use of the internet.

Such workers should also be facilitated to adjust these passwords to those that can be easily memorized without compromising its strength. This aims at lowering the chances of forgetting them or writing it on notebooks or on the computer. Successful implementation of this measure will go a long way in guarding against malware attacks and inadvertent disclosure of company information. Additioonally, the above measure will mitigate insufficient authentication controls especially in large corporations where a number of employees share passwords. Surveys have shown that up to 40% of various company workers who share passwords are not supervised (Cisco4).

If this measure is implemented, it would be hard for an attacker to gain access to many servers because the measure discourages use of a single password to many systems. It should be noted the main aim of password security policy is to reduce the incidence of hacking by creating unique passwords for every account or site used by the company employees. Password security policy also requires that network administrators periodically change all the passwords. Workers Training on Malware Prevention and Containment Studies have shown that most workers have absolutely no knowledge on malware. The best they can do is to report that their computers have ‘ stopped’ working in the event of a malware attack.

They have no knowledge on how to grade the various forms of malware, leave alone how to isolate and disinfect them. It’s therefore highly encouraged that Companies empower these workers by training them on the various malware manifestations and how they can be identified and contained. The most effective way of training is introducing the various examples on a secured computer and using them to train the employees on the step by step containment process. In addition to this training, all workers should be encouraged to regularly scan their computers and other devices like flash disks. The company must also ensure that modern antivirus and antispyware is installed in all the company’s computers and that they are regularly updated. If implemented diligently, stuff training and observance of safe browsing culture would go a long way in protecting the company’s data from malware activities and attacks.

Safe Massage and Email Handling This measure seeks to reduce phishing, cross site scripting and site request forgery attacks. The leading social network sites like Facebook and MySpace have suffered a fair share of phishing and cross site scripting as well as a number of forgery request attacks on their networks (Timm 14). The main trigger points of these attacks have been known to be company and workers’ private emails and online correspondences. Therefore, there exists urgent need to implement safe message handling policy. This will be both for the company and workers’ online activities. Safe massage handling is a security measure that guides workers on how best to safely use the internet while receiving and answering emails and messages.

This security measure prohibits workers from receiving messages without scrutinizing them to ascertain their origin. It requires all workers to desist from clicking on any suspicious links found in messages until they are sure of the sender. The measure further warns the workers not to be too intimate with online acquaintances because not all messages are from them. Special attention is called for when any worker receives a message that asks them to take any form of action. In such cases, safe message handling requires the worker to study the message contents with the aim of ascertaining whether the purported sender could be genuine and up to no harm.

Incase the worker doubts the validity of the message, the best way forward would be to contact the sender either by phone or physically to allay the concerns. In the event that such messages are confirmed to be an attempted phishing attack, the network administrator should forward them to antiphishing sites for further action. Safe Browsing Practice as a Mitigation Measure for Cross Site Scripting and Cross Site Request Forgery Both cross site scripting and cross site request forgery are some of the security threats that are not associated with the workers' behavior. They are, rather, associated with browser settings and browsing practices. Safe browsing practice is a security measure that seeks to limit malware attacks and data loss occasioned by unsecure browser settings.

Most browsers have add ons that facilitate or aggravates malware attacks. This measure encourages workers to disable browser add-ons like the JavaScript, Active X and VBScripts. These add-ons are known to facilitate cross site scripting. Additionally, workers are advised to disable cookies if possible. This is because cookies are known to unnecessarily store private information like passwords and login information (Perez 39).

Storage of such data threatens the credibility of the user's private details. A successful malware attack could lead to massive losses as all the stored data in the cookies will be available to the hacker. This mostly happens without the knowledge of the user which makes it even more disastrous as the user could be opening more secure sites like online bank accounts without knowing that this information is being tapped. In addition to safe browsing practices, workers are encouraged to install firewalls and remove any cross site request forgery attack aids like avoiding numerous active sessions and overstaying their sessions on secure sites. Lastly, safe browsing practices encourage workers to ensure proper logout after every web session.

Elaborate Privacy Policy This security policy governs how workers handle the company’s information.

It seeks to limit both intentional and unintentional data release by the company employees. In the case of intentional sensitive data release by corrupt workers, the policy puts forward a solution in the name of encryption. It requires that all sensitive data be encrypted to prevent possible leakages to the wrong hands. Additionally, privacy policy requires that all employees with access to confidential information should be thoroughly vetted and trained on how to store such information. SANS institute encourages administrators to put in place acceptable privacy policy that prohibits the employees from divulging any company’s data.

It goes further to provide legal recourse in the event of a breach. As well as establishing elaborate steps to be followed in the event of any data leakages or loss. In particular, the privacy policy should clearly prohibit any discussions on the blogs that amounts to data breaches (SANS 7). On the issues of data loss due to genuine mistakes or unintentional blogs or postings on the web, the privacy policy advances the following preventive measures: Workers should desist from getting too intimate with online friends to a point of lowering their guard which may lead to divulging of crucial information. Workers are warned against discussing interesting information about the company with the aim of attracting more friends or greater following on the social network. Workers must exercise outmost professional and ethical contacts at all times.

Privacy policies warn that small harmless information may eventually add up to crucial data losses to the company over time. It's worth noting that privacy policies seek to alter the growing concern that most data breaches are caused internally, mostly through unintentional actions like making innocent comments on a social network about the company's business practices. Based on a 2007 studies on security breaches, over 75% of such cases are caused by insiders (Hirschhorn 18-21). Remedies for online social network vulnerabilities Most social network vulnerabilities are best avoided by observing a strict security policy both by the individuals and business entities. Encryption and Decryption Standards Encryption refers to the process whereby a readable text is converted into unreadable cipher by use of the encryption software.

Encryption is done by the use of algorithms that can only be turned back by the use of a key or a passphrase. There are two standards of encryption: the data encryption standard (DES), and the advanced encryption standard (AES). The data encryption standard is an earlier version while the advanced encryption standard is the latest version. The earlier version has been criticized for its numerous security short comings while the advanced encryption standard is known to surpass minimum security threshold. On the other hand, decryption is simply the process of converting cipher information into a readable text. Example of encryption standards The most common encryption standards used by the online social networks are the Pearson project and the Safebook encryption standards.

Pearson project encryption standard. This is an example of encryption system where the user's data is both symmetrically and asymmetrically encrypted and the decryption key stored together with the accepted user’s information. This would allow access to only accepted friends who have the decryption key. Safemode encryption standard This form of encryption depends on the level of trust an account or profile holder accords to public friends. Under this type of encryption standard, a user decides how much access online friends should get by assigning them with unique keys. These keys determine what information is available to online friends and what is not accessible to them.

Encryption and decryption standards are part of the security measures that protect the integrity of information. This information can be stored or in transit. For example emails make up the data in transit while documents in a flash drive or hard disk represent the data stored. Social networks employ both the data encryption standards and the advanced encryption standards. If data is encrypted, the only way in can be accessed or read for that matter is by using a key or a paraphrase.

The key can be installed on the computer so as to guarantee a seamless correspondence which does not necessarily involve manual decoding. Social networks allow its subscribers to install encryption standards of their choice to guard their online data. Their duty is to simply facilitate the running of these standards and once installed, it’s up to the subscribers to keep their keys safe. Social networks encrypt all the subscriber data in their servers to limit unauthorized access. The only way one can view the information of a friend is by login in using a digital signature which is given by the network sites once the profile owner has approved you as a friend. Individual subscribers of a given network are free to install encryption standard of their own.

This will only safeguard their personal massages with selected friends. In conclusion, most of the security and privacy concerns of social media are manageable and preventable. It only requires the company to do its part of installing up-to-date antivirus and antispyware and back up by training the company workers on how to safely use the internet. The workers need to adhere to the company’s privacy and security policies in using the social media. It is never a solution to ban the use of social media in business operations unless it becomes absolutely necessary.

On a personal platform, subscribers of social networks should exercise restraint in posting information online. They should accustom themselves to keep private information private. Observance of safe browsing is also recommended to all users both businesses and individuals.