Security privacy related threats to social networks information technology essay

Technology, Information Technology

Social Networking Sites have become more popular than ever and because of this reason, the Privacy and Security issues of Social Networking Sites should be examined. In a Social Network, which is a network of personal contacts, a large number of users have access to a common database which is at risk of data-theft from hackers. Social Networking sites take precautionary measures to reduce these threats, but due to the personal nature of the data on Social Networking Sites, most users are at risk of data theft and other Security Issues. On a Social Network, a user can make a Public of Private Profile which can be shared with other users and used to contact and make information available to other users.

Privacy and the Access of Information

When posting information on a Social Network, there are various settings, to authorize which contacts can see this information. Apart from contacts, parties Collecting Personal Data include. Advertisers who wish to attract more clients by gathering data about their behaviorThird-party software developers who enhance user-experience by personalizationIllegal parties include: Identity thieves who gather information directly from the user’s account or indirectly from another account. Hackers and Developers of Malware, Adware and VirusesThird-Party Applications on Social NetworksThird party applications interact with the social Network without being part of the whole network. These applications may take the form of quizzes gams etc... for recreational and education purposes.

Privacy Recommendations of Social Networking Websites

There is a variation in the levels of privacy of different websites. While some encourage more information to be provided, such as Name, Address etc... on Facebook, others encourage anonymity.

Ethical Concerns

There are a lot of ethical concerns here, about the exact extent of information which is made available by the sites to outsiders. The methods by which information can be leaked and how this can be minimized are provided in this essay along with the laws dealing with these. Unfortunately this is a built-in threat which allows third parties to gain too much information about clients. One ethical issue is the method of communication through Social Networks and the profiles used which is usually like SMS language and doesn't show the true identity of the user. Many people now complain that this is limiting their Social interactions.

Social Issue

According to Kizza (2007, p. 316)fake user profiles become a major threat to the social networks and the users. If someone is maintaining two or more user profiles in the same social network, then eventually this social issue will arise. And also this is known as multiple personality; where a particular user might ghost around his or her friends using different and unknown user representations. Most Social Networks try to ensure that the level of security on their networks is high, but usually personal information can be easily leaked. Predators use Social Networking Sites to hide behind a false identity and trouble others. As of 2009, Myspace had evicted 90, 000 sex offenders

who had done this. The case of Amanda Todd where a teen's death was caused by bullying on Social Networking sites is an example of a Social Issue. In a study of Facebook profiles at the Carnegie Mellon University, about 800 profiles were studied and revealed that a significant number of people updated their location status on Social Networks, thus allowing others to know their location. The ease for others to know read private messages and email on Social Networks is also a concern.

Security and Privacy-related Threats to Social Networks

The information provided to a Social Networking Site range from Contact information, to Photos to Employment –related matter and demographics. Most users commonly use their profiles to make friends with others easily, and thus the risk of violation of Security and Privacy is high. The rights to privacy and Freedom of Information are thus highly important here. Bott F. (2005, p. 181) In this type of scenario, information such as, PasswordsBank account informationCredit card numbersInformation stored on a user's computer such as contactsEnter the user's machine without his or her consent (ex, through & malware)Haply Aim and result in theft of Social Networking Accounts and identity to log into these accounts. Generally, Social Engineering is used by hackers to gain sensitive data related to user accounts and hack the accounts. Social Engineering is the manipulation of Social Networks in various ways such as posing as another, diverting attention and Phishing. Spamming and Malware attacks are also used against users, to destroy and hack targets. War-Dialing or randomly dialing phone numbers to spot unprotected computers was an early device used by

hackers, but is still effective. This random spotting of Social Networks still takes place through email addresses and directories. Adams, Rachel McCrindle (2008, p. 377) usually, an attacker will try to make contact with a user or directly steal his valuable details. Tracking Software can also be used for the same. At the same time, those who are part of a node or group with similar interests may be hacked. Usages of third party applications such as quizzes or games, fake profiles, fake websites, spam are other avenues used by hackers. Koobface and Twitter worm are some of the more serious viruses which could affect Social Networks. This sort of threats propagates across networks.

Privacy Policies and Settings

Although a Terms of Use Policy is provided to the client by most Social Networks, these allow for more violation of privacy such as Storage of Data and sending information to Third Parties. It is important for the client to read such terms before entering a contract. Doing this can prevent future complications and become a defense if a problem appears. Poor Privacy settings of accounts such as the facility in Facebook to let only some information be available to a certain group of people, is also a leading cause of problems. If these details are customized properly, data leakage can be minimized.

Professional issues

Employment-issues are a major concern when it comes to employee-privacy mainly, since Social Networking Sites are checked by employers regularly by 1 in 5 employees, according to CareerBuilders. com, in order to seek

information about employees. This is controversial since it could be discrimination, if a person is judged according to his Social networking life. Social networking has major impact on almost every profession. According to Bacon and Lee (2010, pp. 533-534) most of the UK employers don't have proper social networking user policies for their employees, it is estimated as 76%. Most people had lost their jobs due to violation of professional code of conduct. According to medical code of conduct doctors and nurses can't publish pictures to the internet posing with patients; in fact it is violation of patient's privacy.

User-anonymity on Social Networks

Many Social Networkers sometimes choose not to provide their real identity on the networks, by providing no details such as name, Age etc... or providing pseudo details. Some of these categories are, Socially conscious peopleProfessional who do not like to reveal themselves on networksIndividuals with Medical Conditions who seek help but wish to remain anonymousBloggers and Activists who engage in discourse about sensitive matters. Victims of AbuseThis sort of Anonymity puts the account holder at less risk, but increases risk to others from hackers and such other malicious people who do the same.

Legal Issues and Aspects

Considering the Legal Aspects of Social Networking related to Privacy and Security, the following apply. These are the only ways to gain compensation if there is any breach of Privacy or security. Laws concerning leakage of unauthorized information such as trademarks and trade-secrets are serious

and the same laws which apply generally to these fields apply to the electronic field as well. Defamation Issues- If a person’s reputation is destroyed on the internet or cyber-bullying or other such malicious activities take place, the basic laws against harassment apply while privacy laws also apply. Human Resources Issues- In many companies, as mentioned before, profiles of employees on Social Sites are reviewed and this is sued to measure a person’s qualities. But this sort of activity is a type of discrimination under law and may be take up at court. Computer Fraud and Abuse Act (CFAA), 18 U. S. C. S1030 et seq. 18 U. S. C. S 1030 states that, whoever logs into a computer system without proper permission and obtains secret information and private information from any protected computer is liable for punishment. In the UK, Unauthorized Access to Data and Unauthorized Modification of Data are prevented by the UK Computer Misuse Act. Rachel McCrindle (2008, p. 388)Unauthorized Access and the Computer Fraud and Abuse Act, N. Y. L. J., Oct. 12, 2010" The Computer Fraud and Abuse Act targets unauthorized hackers.

Institutional concerns

When institutions join Social Networking Sites, there are at risk of plagiarism and theft of data. Schools, Libraries and Government Agencies have provided information to Social Networking Sites, but many are aware that sensitive information is always at risk from outsiders. Libraries are especially complaining that their ethics are violated.

Conclusion

Conclusively, it can be states that there is generally a threat to security and privacy on Social Networking sites, but this risk can be reduced by individuals by taking precautionary measures and increasing the privacy settings of an account In the meantime, the Social Networking Sites too are taking major efforts to minimize the above threats by increasing security and awareness about their system.