Vanessa Cisneros

ISM 4323

October 11, 2016

Social Media Security

Social media has become inevitable in the evolving digital arena. It is important in modifying the way people interact with associates and friends. Although social networks are playing a considerable role in people's everyday lives, they are a source of security threats such as identity spoofing, financial fraud, information forgery and piracy, stalking, online scams, bullying, and identity theft (Newman, 1999). The rising security challenges emanate from the fact that social media users share information unreservedly with disregard for confidentiality. Opportunities for identity theft are predominantly on the rise following the growing global use of social media. Identity theft refers to situations where criminals gain access to and use of people's personal info such as insurance information, bank account, social security, and credit card numbers to procure services or goods fraudulently.

Identity theft in social media has become an everyday occurrence. Millions of people suffer from identity theft every year causing them to incur lots of money and spend many hours to have their identities repaired and recovered. Several factors are responsible for the escalating pattern of social media fraud and theft. To begin with, social media sites such as Facebook, YouTube, and Amazon target advertisements as their main sources of generating revenue. The advertisements usually base on personal information, thus requiring registering users to fill in loads of personal information. Nevertheless, there is limited government regulation, incentives or industry standards to

educate online users on matters of identity protection, security, and privacy. Consequently, the users become vulnerable to identity fraud and theft.

Online sites have a lot of private user information, which increases their vulnerability to both inside and outside attacks. For instance, Google has recently acquired rights to the use of an algorithm that rates the user's influence on social media. The use of this algorithm is likely to draw many active participants.

Crime opportunities are responsible for identity fraud and theft in the social media. For example, criminals can use consumers' social updates on Facebook, Twitter, Instagram, and other sites. If an online user posts that they are going on vacation, they may set themselves for burglary, robbery, or assault. Besides, video- and photo-sharing platforms like YouTube and Flickr grant criminals a profound insight into an individual's life, family, friends, and property, thus making it easier to stalk or steal the person's identity. Usually, individual profiles on the social networking platforms have people's full names, date of birth, hometown, relationship status, location, email address, and many more, which increase the individual's vulnerability to abuse and identity theft. As Lewis (n.d) states, 95 percent of Facebook profiles contain at least one app that can be used for criminal and malicious purposes.

In spite of the risks associated with the social media, most people do not carry cybercrimes with the seriousness they deserve. This is because social media users do not realize how real online threats are until it is too late. Hence, following the countless genres of cybercrimes being committed in the current digital sphere, individuals need to protect themselves from online crimes such as cyber identity theft, cyber bullying, and fraud. Although there are innumerable laws drafted to help in protecting the consumers,

the only authentic way to make the internet a safe arena is to assume all the necessary measures to protect individual identity. The initial step in protecting oneself from identity theft is diligently securing personal information (Lipton, 2011). Online accounts need to have strong passwords, which incorporate both upper and lower case letters along with a combination of symbols, non-letter and numerical characters. The passwords should not only be unique, but they should also be different for different online accounts. Besides, one should make it a routine to change passwords after some time to ensure that criminals do not have entry into the online accounts.

Online users must be safe with their status updates to protect themselves from identity theft. Often, online participants innocently post status information that would reveal the info that thieves require to steal their identity. For instance, one may post a photo that reveals their valuable info such as the time of taking the picture, the kind of Smartphone or camera used to take it, where it was taken, and current activity, hence disclosing too much information to potential thieves. Posting such information may make it easy for stalkers to find someone. As well, once someone posts the information online, it no longer becomes private, and it can fall into the wrong hands. Therefore, the more a person posts, the more vulnerable the information becomes because criminals can gather as much info of the person as they want. For that reason, it would be safer if online users put fake details on their online accounts to enhance their safety. Besides, they need to avoid indicating landmarks and street signs while uploading pictures. Moreover, people must always be selective with the statuses they update online, avoid statuses that reveal locations, and post pictures after returning from vacation.

Social networking, a common activity among hackers, increases susceptibility to identity theft. The hackers interpolate malicious codes that can steal someone's identity, obstruct personal information, and inject viruses into the user's computer. By hacking one's computer or social profile, they steal all your information. The hackers may also use shortened URLs to trick users into accessing harmful platforms where they can easily compromise personal info. A common way that they use to access someone's social media account is providing a link and requesting the user to click on it. The link redirects the user to a page that looks real, and the user enters personal information, hence granting the hackers entry into the account. Therefore, online users should avoid clicking on links unless they can recognize their sources. To determine the authenticity of a link, the user can use link scanners to check the safety of the URL.

Despite installing the highest security settings on networking sites, information can still leak. The apps, websites, and games contain the users' private information. Once the users browse a website, cookies that track one's activity from one site to another mark them. To deter these platforms from tracking one's activities, the user should enable the out of tracking feature. Additionally, they can clear the cookies and cache on the browser often to avoid imminent problems.

A major risk in online platforms is revealing one's location. It allows criminals to know the whereabouts of a person. For instance, people revealing that they are checking in at the hotel or airport might appear innocent but criminals make use of social media to know where a person is at some given time. Therefore, online users should activate their privacy settings while using location-sharing apps like Facebook. They ought to ensure that the location remains hidden and the GPRS feature on their phones is turned off.

There is a myriad of security risks affiliated to social media platforms. Identity theft has become a major crisis that can pose lasting impacts on a person's life. Social media platforms have become crime scenes because users put lots of confidential information on them. For that reason, because the social media is indispensable in the digitalizing world, users need to be vigilant because there are numerous ways that criminals want to hack user information for their personal gain. Online participants must enhance their online security and safety by embracing measures that prevent their information from landing into the wrong hands. Before using social media platforms, users need to be acquainted with the risks and best practices to protect their information and their systems.

References

Lewis, K. (n.d.). *How social media networks facilitate identity theft and fraud*. Retrieved on October 11, 2016.

Lipton, J. D. (2011). Combating cyber-victimization. *Berkeley Technology Law Journal, 26*(2), 1103-1155.

Newman.J.Q. (1999). *Identity Theft: The Cybercrime of the Millennium*. Port Townsend: Loompanics.