Social Media Privacy and Security – Developing Guidelines

Carlos D. Santiago Bonilla
Master of Engineering in Computer Engineering
Advisor: Nelliud Torres Batista, DBA
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

***Abstract* —** *Society over that years have seen an increase on how technology impact the user daily lives. The average user spends around 11 hours each day connected to any form online. Technology has become a basic need in the 21 century users can access from a wide range from live tv, newspaper and even researching on how to perform different types of task. The average daily user spends around two and half hours on social media. Most of social media requires an exposure to detail about private life when creating account for example a: profile picture, birth day date, full name and accepting a user agreement. However, a couple of question have raised over the use of the social networking and the risk it involves. How do we know that the person that created the profile is real? What information the user provided is made public? What guides should I use for maximum protection using social media?*

***Key Terms* —** *Information, Privacy, Security, Social Media.*

OBJECTIVE

Evaluate each top social media website and how each one affects the user private life and the security of that user confidential information gets exposed. Design guidelines to utilize the internet in the safest possible way.

INTRODUCTION

Society over the few years as seen an increase of usability and accessibility over the internet. The tool that's was first designed for military purpose is now serving as a mechanical way to perform globalization expanding business from micro to macro establishment with a couple of clicks away. Social media is defined as "online tools and websites that encourage people to interact with companies, brands, and people (including celebrities and journalists) and form communities by creating, publishing, and sharing content. Social media is a two-way communication stream, whereas with traditional media, messaging is published through a one-way communication stream to the masses, e.g. radio, television and newspaper" [1].

Social media have come a long way in recent years many platforms have been created to serve different types of needs with different approaches to each user. Some example of social media are Facebook, LinkedIn, Twitter, Instagram, Snapchat, WhatsApp and Myspace. Each of these social media platforms requires to provide personal information that for some users are considered a great vulnerability.

Social media have different types of approaches one is the ability to establish communication with anyone around the world that has a connection to the internet. One example of this approach is the platform called Facebook lets the users communicate with each other using instant messaging. Some other features include buying and selling groups, communicating with family member using instant messaging and even use the platform to inform about different events that could be of interest to the user. On recent update users can perform video chats and calls using devices. Another approach in a more of a business career area dedicated to expanding what is called in the industry *Networking* utilizing the platform called LinkedIn to get users or human resources to acknowledge the user skill and educational career that could lead to plausible job offer from companies.

Another social media class type can be a mix of instant messaging with sharing photo and video content. The platform called Snapchat does exactly that, lets the user share photo or video with a time

limit so another user can see the original content. In recent updates the company decided to integrate a world map that with the location services in our devices it can pin point where we are and where our friends are located.

However, with great benefits social media brings in to modern society so it brings a lot of recurrent problems to it. The main problem social media brings is the accessibility that anyone must create an account in any type of platform it only requires a few information data with no verification of the information that was provided to create the account. Inclusive, many other problems that have risen over the past years and technology keeps evolving making it easier to perform scams but also easy to detect the scam and report it to the local authorities.

ANALYSIS

Examine the different types of risk a user has on social media. Explore how the exposure on social media has affected the users with less knowledge. Identify the types of risk and how to avoid them. Analyze one of the biggest cyber-attack on social media.

Exposure on Social Media

The increase in scams and identity theft has increased self-thought awareness like public authorities. According to CNBC news "Some 15.4 million consumers were victims of identity theft or fraud last year, according to a new report from Javelin Strategy & Research. That's up 16 percent from 2015, and the highest figure recorded since the firm began tracking fraud instances in 2004" [2]. Identity theft reported by the CNBC in 2015 alone a 15.4 million of users had some type of identity theft made online or phone. The statistical report presents a 16% increase in identity fraud comparing with 2015 with 2004. The estimated cost in 2015 for all affected user translate into 15.4 million of dollars just for that one year alone.

Different types of social media are part of a daily life of any individual regarding their form of use or platform of preference. However, the majority of social media platform give a tutorial on how to protect one's identity on social media. Most of the times a tutorial is giving on the first lunch of the application or first time registering on how the platform works and how each button function not on how to prevent any time of fraud or scams. On the social media called Twitter a type of fraud is particular where the person creates a fake account to attack different persons "A common scheme is for a scammer to create an account then follow or direct message hundreds or thousands of other users. Each time a user is followed, they receive an alert with a link to the scammer's profile. The profile often contains links to malware or phishing sites" [3].

Social media has become a target for people to steal information about other people without having to become to much exposed by placing different types of traps or cyber-attacks. Most of the social media know about their platforms are used to perform and commit fraud to other users and some updates are provided to fix most of these issues. Facebook over the course of these year have admitted that in their platform some users have created false news providing mis guidance to other users that read the news without first verifying the authenticity of the news. According to Facebook "We've found that a lot of fake news is financially motivated. These spammers make money by masquerading as legitimate news publishers and posting hoaxes that get people to visit their sites, which are often mostly ads" [4].

Risk and Threats

One of the scams that is the most common is called Dating Scams and it consist of a person or attacker playing the role of a lover or someone with great interest in the target. The webpage Security Intelligence defines it as "is an internet scam in which a cybercriminal creates a fake online profile to seduce a victim into a fictitious online relationship usually to get money or other benefits from the victim" [5]. Usually the attacker come from dating application and social media where they require the victim to provide personal details, money or any type

of valuable item that can be sold for a great deal amount of money. The process on how to perform a Dating Scam is easy just by creating a false profile with a false profile picture and study that persons favorite things to do and interest and become the perfect soulmate to begin extracting information.

Another common scam is called Profile Hijacking, and this becomes more elaborated than the first mentioned "cybercriminals often use the attributes and details of real people like their photos, hometown and occupation to set up profiles pretending to be that person [5]. The profile hijacking can be done by simply creating a fake profile with a fake email, profile picture and name. First the attacker begins contacting random people to be accepted into the account. The attackers then start gathering information about the victims or just by creating a fake profile. The victim not knowing the profile is a fake one attacks can be gathering information, monetary favor can be asked or can even be blacked mail. Once information is gathered from each user a new victim is in process.

Also, a major type of scam is a Message Chain "Chain letters are messages sent to a huge number of people, asking each recipient to forward them to as many other people as they can" [6]. These messages are sent to many users claiming different types of things and when the victim enters of the external link personal information is extracted from the user. Some messages include being the winner of a lottery ticket claiming that you have won million and millions of dollars that they just need to verify a couple of information. One thing that the user needs to realize if a ticket was bought. Some threats presented in chain messages are online fraud, virus, identity theft and negative impact on the victims.

The use of Data Mining in the social media has become a problem in the present does not only affect the victims but also the people that knows that victim. According to Security Intelligence the attacker use type of built in application "cybercriminals will include links embedded in the quiz that can steal information from your personal accounts. Once these criminals have your account information, they can use it to lure in other unsuspecting victims" [5]. Some attackers create a certain application to extract all the information possible without the users knowing what is going on. One example of these application can be the Quizzes that are made on Facebook regarding movie character, sport players and many more where usually they store the user information and their contacts allowing to send different investigation to other user to compile more information. Some even can say that in one scam attempt are multiple ways on getting scam for example shorting URL to get the user to malicious website, being contact by fake profile and many more to mention.

History on Scams

One of the Biggest social media scam was reveled back in 2017 although some say it was by 2008 in the beginning of social media one website was above all the other competitors called Myspace in the 2000.

According to Innovation & Tech Today by the 2018 Myspace reportedly announced the 1 billion benchmarks of users around the world "In March of last year, the hacker "Peace" claimed to have access to the email addresses, usernames, and passwords of approximately 360 million Myspace users. Based on analysis of email domain frequency, the actual hack is more likely to have occurred back in 2008, with Peace just now deciding to make the breach public" [7].

METHODOLOGY

Inspect the types of vulnerability different types of social media platform have. Analyze how easy is for a hacker to get in any type of platform and perpetrate their attack. Evaluate the default setting that a social media provides and the danger they represent. Create a conscious among the reader about what they share on social media. Develop possible guidelines for a safer social media interaction.

Vulnerability

One major thread in the social media plane are how easy a cyber-attack or scam can be done the next

photo the minimal user information required to create an email account. However, the information that is provided with the email account is necessarily verified by anyone.

Figure 1 shows how simply creating an email is in this case is a Gmail account only requires a first name and last name with a password. The next step is very straight forward day of birth and gender. Completing these steps and accepting the service agreement the email has been created without verifying any type of information.

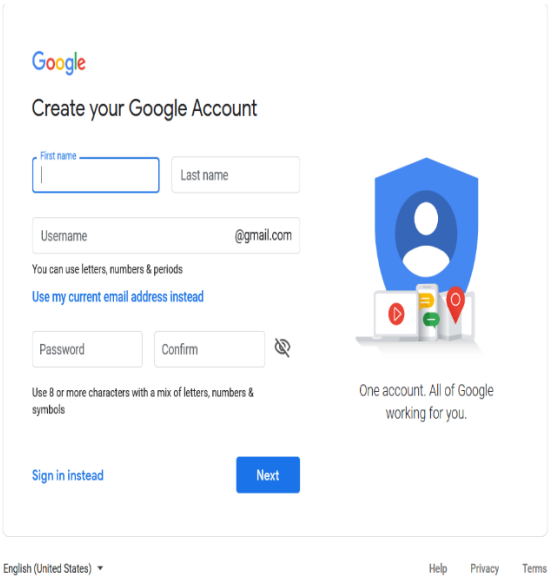

Figure 1
Creating Gmail

Creating a social media account is a straight process without the validation of any credentials. Usually the platform asks for name, email and a password.

To create a social media account on Facebook, see Figure 2, it only needs first and last name, email address, password and a day of birth. Again, none of this information that is provided is not being validated by someone nor the profile picture the user decides to publish.

Some of the possible danger a victim can be put through is taking someone else picture, name or even start making a profile of the person and pretend that they are the real person and these type of situation can be used to get more victims to continue committing the crime.

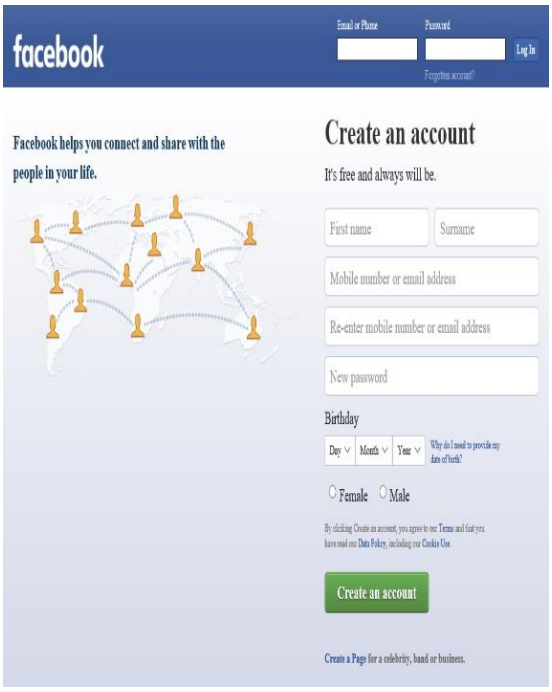

Figure 2
Creating Facebook Account

Social media and email accounts, both have a set of pre-configured setting to quickly utilize the function, however these types of setting that have been pre-selected and considered as a default are all in the hundred percent safe. Two examples will be presented the first case of default setting is on Facebook the user gets a basic tutorial when the first enroll on the website however the user does not get a tutorial on what each setting means and what types of risk do they present to.

The private settings used as default for the social media called Twitter does not automatically choose a two-way authentication, tweet privacy is not checked by default meaning tweets or post will be made public and finally Twitter adds the location to tweet or post the user just made since it's a default setting.

Other social media as Facebook, Twitter (Figures 3 and 4) and Instagram have the same privacy default settings making privacy harder. Plus, the majority of these sites does not include a tutorial on where are the settings, how to change the settings and explain what each setting is being referred to before making any choices.

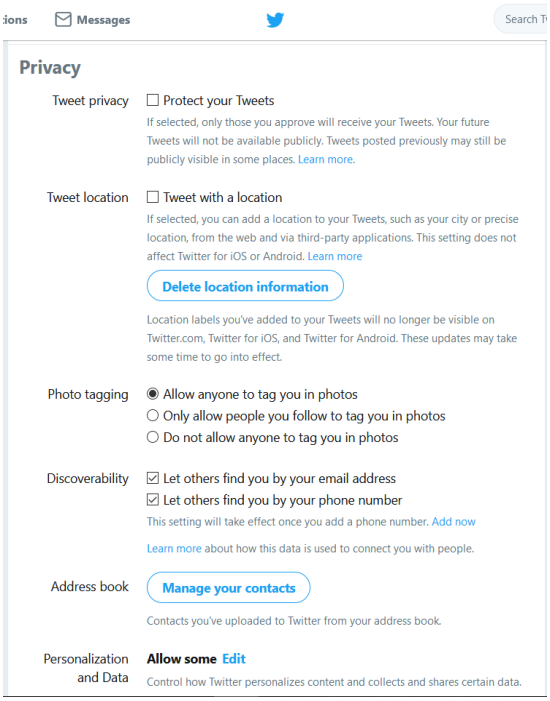

Figure 3
Twitter Security and Private Settings

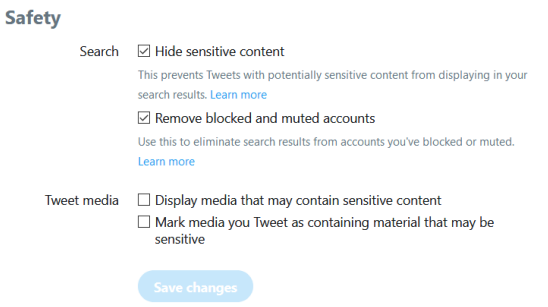

Figure 4
Twitter Safety Setting

Location Services Risk

The application called Snapchat is a social media site with a few variations photo shared with contacts get deleted time limit is reached, the user decides what contact gets the content and monitors how the individual uses the content in the time limit however the privacy settings has been set so that anyone contact the user , see the user story and find them on the snapchat map (Figure 5) without the knowledge of the users their privacy has been reduced to nothing anyone can see where the user is and what the user is doing without having to leave any trace that the user is being watch.

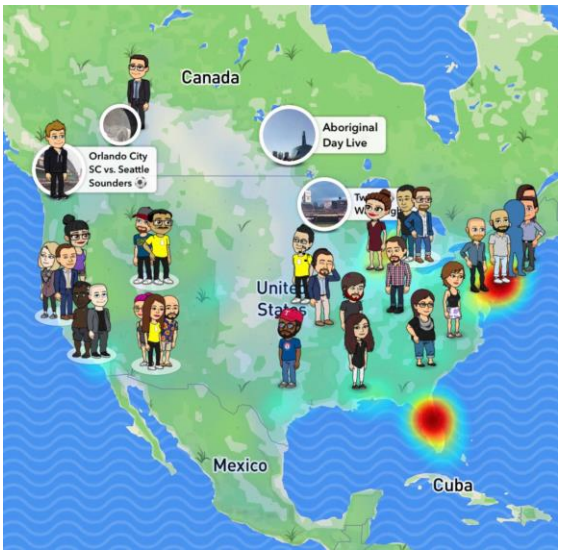

Figure 5
Snapchat World Map

Many of the application that comes from social media have the setting added for the location services. The phone location services are design to find the geolocation of the user around the world these feature lets the attacker know where their victims are if the users are not responsible on how the use the location services. The attacker will know where their victims will be at any time.

Culture

The culture of living in a modern society where technology has been a part of a daily life of each person. Always remembering that a social media page is used and modified as the user needs and the user controls the contents in his own social media page. Even though the user controls his social media the aspect of privacy and security settings have a pre-determined setting for the users that the original user can modify them. According to Gwendolyn society post about "Your high school friend sharing photos of her kids, your cousin complaining about physical illness, your colleague opining on politics, your friend posting funny animal videos" [8].

However social media is not all negative it has helped many user stays connected with other users around the world. The webpage called Business to Community states what is shared on social media are "43% Pictures, 26% Opinions, 26% Status Update of

what and how they are doing, 26% Links to articles, 25% Personal recommendations of things they like, 22% News items, 21% Links to other websites, 21% Links to other people's posts, 19% Status update of what they are feeling, 17% Video clips and 9% Plans for future activities, trips and updates" [9].

At a professional level user who are employed by a company do get research by the company staff. A social media profile serves as a representation of that users' interest and discomforts "Employers have long done various forms of screening, including criminal background checks, on prospective employees. The Web and social media provide a vast new collection of information on job applicants. Search companies can have a policy that they perform social media searches only if the applicant consents" [10]. Social media in the present represent a major turning point in our daily life it has the ability to change the user possibility of landing a position at a company either for good or for bad.

Social media is not all about danger and risk and being exposed clearly some threats that are on the web but with safer conscious use of the social media the user can use it as a communication system. In social media the user can express their thoughts, open to a debate, find other user with similar interest, find old colleagues, able to communicate with other user at long distance and share a moment or an event in the user life's with others.

Guidelines

A major problem has come to arise on the web on how many people have been affected with cyber-attacks. Cyber-attacks that can affect any user of the web from cyber bullying, cyber stalking and many other. Schools or evening developers that made application or webpage for social media do not provide guidelines to a safer and healthy use of the web more precise social media websites. The guideline should always try to protect the user at the most.

A quick search using the web for secured or safety guidelines for social media gives the user a quick background on general safety on the web. However, it lacks on how to act on specific types of situation and different types of platforms social media is being accessed.

The development of a social media guideline should include. A tutorial regarding where the privacy setting is located and what each option allows what to make public and what to keep in a more private life. Give the user a basic introduction video on the risk of publish any type of post on social media that once something goes on the web it stays on the web forever to explain how cautious people should be on what to post in their social media websites. The risk of getting contacted by people they do not even know who they are.

Also, orient user of using third party's application with their social media and what type of information will be shared between the developers and the user. Explain the risk of using a public Wi-Fi Spot or using a public computer for personal use. Establish some type of golden rule on what type of situation has gone out of hand and it is time to contact local authorities to protect the user. According to Emerson College a few hints and tips "The Internet is open to a worldwide audience. When using social media channels, ask yourself: Did I set my privacy setting to help control who can look at my profile, personal information, and photos? You can limit access somewhat but not completely, and you have no control over what someone else may share, How much information do I want strangers to know about me? If I give them my cell phone number, address, email, class schedule, a list of possessions (such as my CD collection), how might they use it? With whom will they share it? Not everyone will respect your personal or physical space, what if I change my mind about what I post? For instance, what if I want to remove something I posted as a joke or to make a point? Have I read the social networking site's privacy and caching statements? Removing material from network caches can be difficult. Posted material can remain accessible on the Internet until you've completed the prescribed process for removing information from the caching technology of one or multiple (potentially unknown) search engines Have I asked permission to post someone else's image or

information? Am I infringing on their privacy? Could I be hurting someone? Could I be subject to libel suits? Am I violating network use policy or HIPAA privacy rules?".

The proposed guideline for a safer and private social media is the following.

- User of social media under 18 should consult with legal guardian
- The personal information and content when creating the profile since it will be public
- Verify privacy and security settings
- Do not add another user you do not know in person
- Do not open external link
- Photos in social media are public
- Post will be available to everyone one to see or your contacts
- Joining groups also let the group leader to see the user information
- Do not disclose private information
- Ask permission to re post
- Ask permission of another user when sharing a photo
- Report any miss use or conduct in appropriate in social media to the corresponding authorities
- Once posted on the internet will always be kept in the internet no way of deleting it
- Verify the post does not break any law
- Do not perform scams
- Respect other user contents
- Updated antivirus

CONCLUSION

In the 21st century society has changed their communication lifestyle from phone calls and written letters to send instant messages, email and video calls. Social media has become one of the most import way to stablish communication now and days whenever a catastrophic event happens the first thing people do is post it or comment on it on their respective social media platforms. A sense of security and online protection should depend on each user on making the web safer for everyone to use. However, the ways attacker hurt their victims have changed from also getting victims on the web these victims can come from cyber bullying cyber stalking and even steal personal information.

The guideline will provide for a safer and secure social media would contribute a lot of help to the society that is shifting from manual task to online tasking their majority part of their lives. A user can be safer and more protective if they followed the proposed guidelines and be open mind minded to judgment. The guideline is not a complete protection since vulnerability and exploits are discovered each day however it can aid the user to be safer than in the past.

FUTURE WORKS

Updating the guideline and adding possible scenarios so people can identify themselves to. Include a tutorial on for each social media and how to set up the best setting for keeping a safe and secure social media profile. Add warnings to possible post that can in some way affect the user in any way possible. Establish relationship with developers to be part of introductory tutorials. Join different government agency to spread conscious over different user and the risk that is presented in modern social media live.

REFERENCES

[1] K. Hong. (2019). *What is social media?* [Online]. Available: http://www.seniornet.org/index.php?option=com_content&view=article&id=713:what. [Accessed: Apr. 26, 2019].

[2] K. B. Grant. (2017, Feb. 1). *Identity theft, fraud cost consumers more than $16 billion* [Online]. Available: https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html. [Accessed: Apr. 26, 2019].

[3] National Consumers League (NCL). (2012, June). *You on Twitter? So are scammers* [Online]. Available: https://www.nclnet.org/you_on_twitter_so_are_scammers. [Accessed: Apr. 26, 2019].

[4] A. Mosseri. (2017, April 7). *Working to Stop Misinformation and False News* [Online]. Available: https://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news. [Accessed: Apr. 26, 2019].

[5] J. Goodchild. (2018, Aug. 9). “What Are the Seven Biggest Social Media Scams of 2018?”, in *Security Intelligence*, [Online]. Available: https://securityintelligence.com/what-are-the-seven-biggest-social-media-scams-of-2018/. [Accessed: Apr. 26, 2019].

[6] BullGuard. (2019). *How dangerous can chain letters be?* [Online]. Available: https://www.bullguard.com/bullguard-security-center/internet-security/internet-threats/chain-letters?lang=en-in. [Accessed: Apr. 29, 2019].

[7] I&T Today. (2018, Aug. 16). *Here's the hacker behind the largest-ever social media data breaches* [Online]. Available: https://innotechtoday.com/heres-hacker-behind-largest-ever-social-media-data-breaches/. [Accessed: Apr. 26, 2019].

[8] G. Seidman. (2015, July 2). *What Can You Learn About People from Facebook?* [Online]. Available: https://www.psychologytoday.com/us/blog/close-encounters/201507/what-can-you-learn-about-people-facebook. [Accessed: Apr. 29, 2019].

[9] B. Hutchins. (2014, Aug. 14). *What & Why People Share on Social Media (Infographic)* [Online]. Available: https://www.business2community.com/infographics/people-share-social-media-infographic-0975231. [Accessed: Apr. 29, 2019].

[10] S. Baase, *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology*, New Jersey: Pearson, 2013.