Social Media Privacy and Security – Developing Guidelines

Carlos D. Santiago Bonilla
Advisor: Dr. Nelliud Torres Batista
Electrical and Computer Engineering and Computer Science Department

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. Most of social media requires an exposure to detail about private life when creating an 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?

Introduction

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 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. 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 to create an account with no information being verified.

Analysis

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."[2]

Different types of Risk and Threats on Social Media:

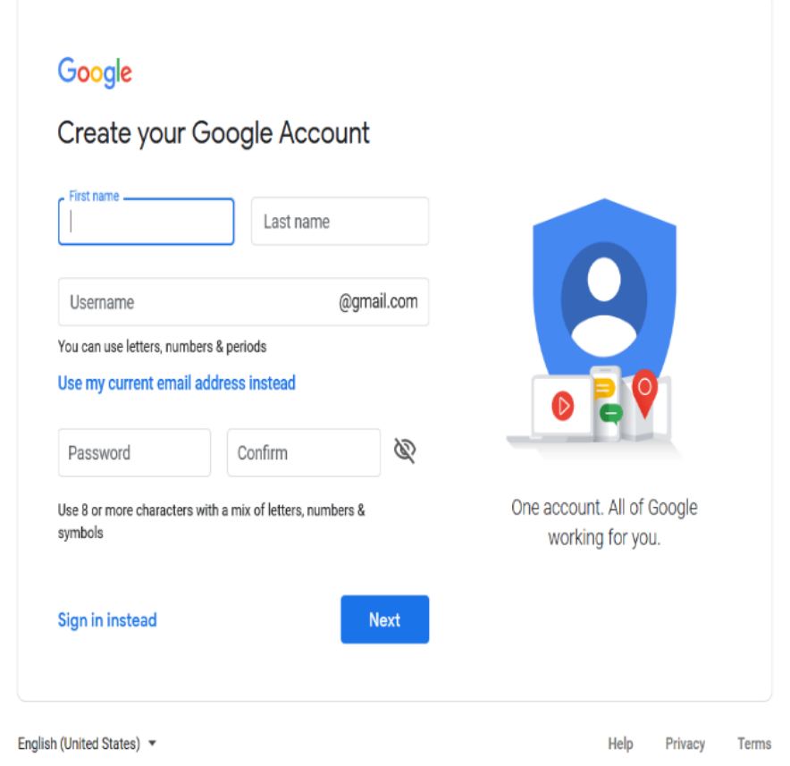
- Dating Scams and it consist of a person or attacker playing the role of a lover or someone with great interest in the target.
- Profile Hijacking uses the attributes and details of real people like their photos, hometown and occupation to set up profiles pretending to be that person [5].
- Message 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].
- The use of Data Mining in social media to extract information and create a profile of each victim

One of the Biggest social media scam was reveled back in 2008, the hacker "Peace" claimed to have access to the email addresses, usernames, and passwords of approximately 360 million Myspace users. [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.

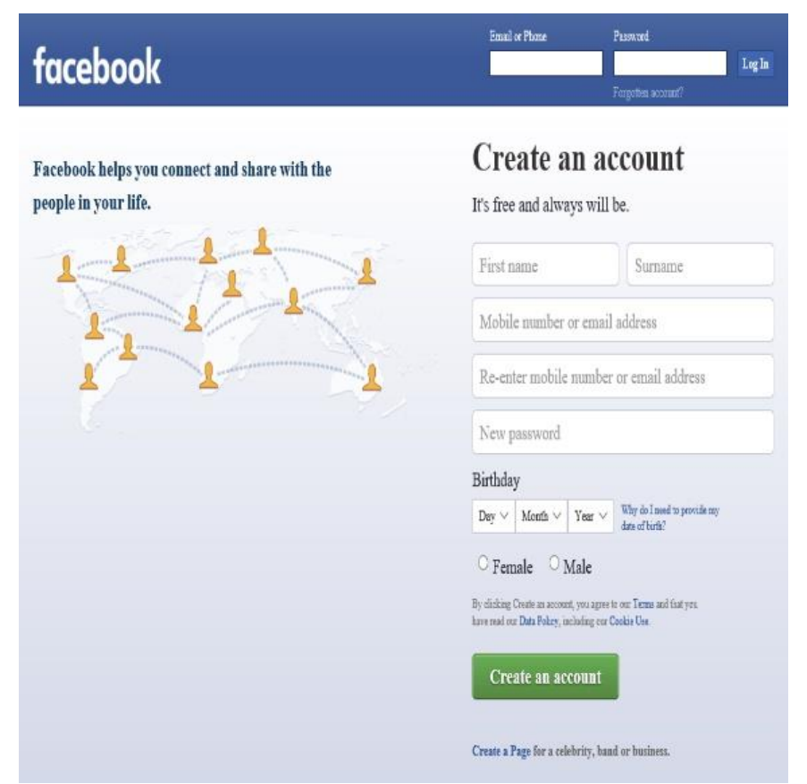
- Figure 1 shows how simply creating an email is in this case is a Gmail account only requires a first name and last name with a password. The next step is very straight forward day of birth and gender. Completing these steps and accepting the service agreement the email has been created without verifying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



Google
Create your Google Account
First name | Last name
Username @gmail.com
You can use letters, numbers & periods
Use my current email address instead
Password | Confirm
Use 8 or more characters with a mix of letters, numbers & symbols
Sign in instead | Next
One account. All of Google working for you.
English (United States) | Help | Privacy | Terms

Figure 1
Creating Gmail

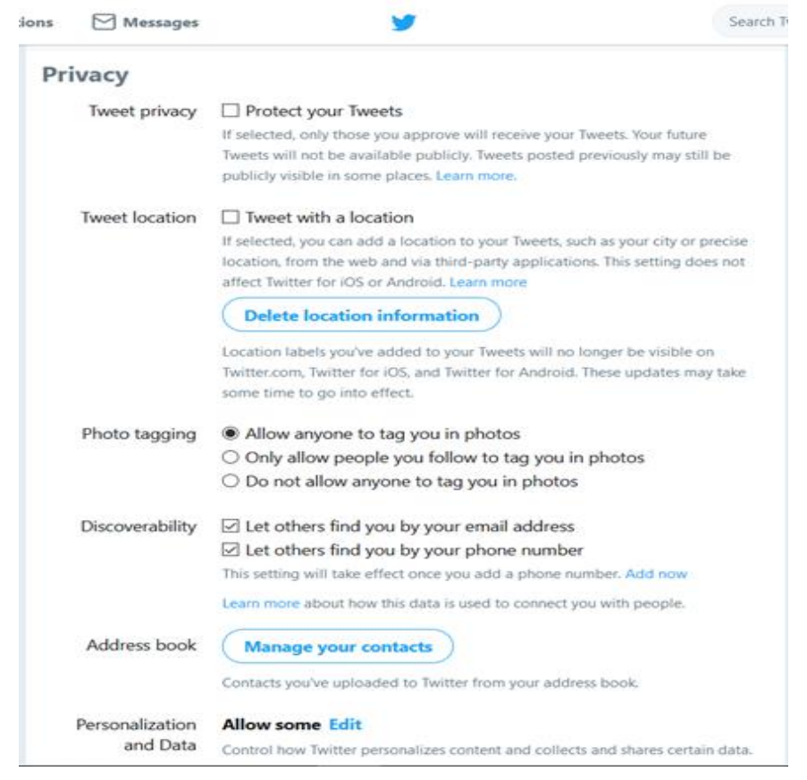
- To create a social media account on Facebook, see Figure 2, it only needs first and last name, email address, password and a day of birth. Again, none of this information that is provided is not being validated by someone nor the profile picture the user decides to publish.



facebook
Email or Phone | Password | Log In
Forgotten account?
Facebook helps you connect and share with the people in your life.
Create an account
It's free and always will be.
First name | Surname
Mobile number or email address
Re-enter mobile number or email address
New password
Birthday
Day | Month | Year | Why do I need to provide my date of birth?
○ Female ○ Male
By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.
Create an account
Create a Page for a celebrity, band or business.

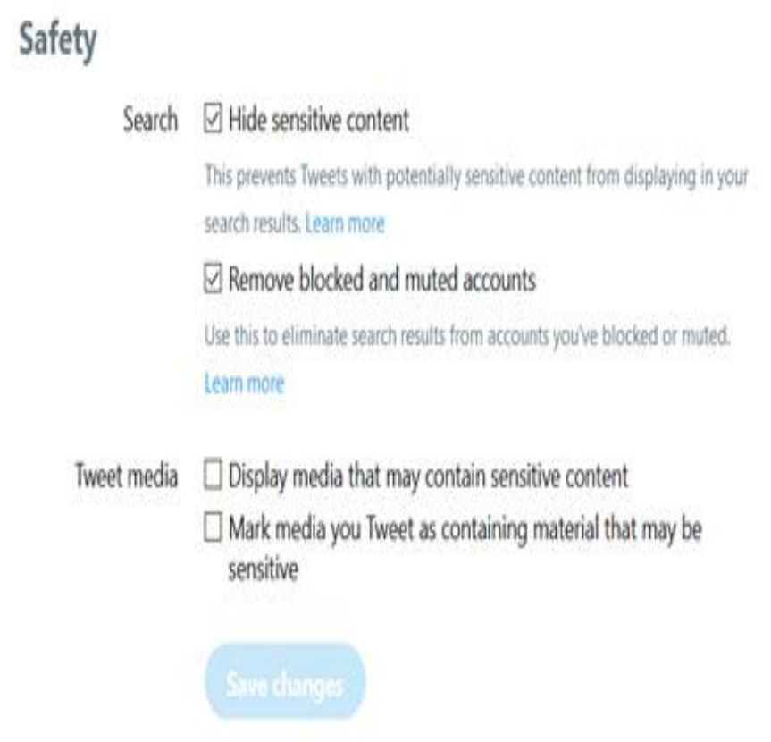
Figure 2
Creating Facebook Account

- 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. Examples shown in Figure 3 and Figure 4



Messages | Search
Privacy
Tweet privacy: □ Protect your Tweets
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.
Tweet location: □ Tweet with a location
If selected, you can add a location to your Tweets, such as your city or precise location, from the web and via third-party applications. This setting does not affect Twitter for iOS or Android. Learn more
Delete location information
Location labels you've added to your Tweets will no longer be visible on Twitter.com, Twitter for iOS, and Twitter for Android. These updates may take some time to go into effect.
Photo tagging: ● Allow anyone to tag you in photos
○ Only allow people you follow to tag you in photos
○ Do not allow anyone to tag you in photos
Discoverability: ☑ Let others find you by your email address
☑ Let others find you by your phone number
This setting will take effect once you add a phone number. Add now
Learn more about how this data is used to connect you with people.
Address book: Manage your contacts
Contacts you've uploaded to Twitter from your address book.
Personalization and Data: Allow some Edit
Control how Twitter personalizes content and collects and shares certain data.

Figure 3
Twitter Security and Private Settings



Safety
Search: ☑ Hide sensitive content
This prevents Tweets with potentially sensitive content from displaying in your search results. Learn more
☑ Remove blocked and muted accounts
Use this to eliminate search results from accounts you've blocked or muted. Learn more
Tweet media: □ Display media that may contain sensitive content
□ Mark media you Tweet as containing material that may be sensitive
Save changes

Figure 4
Twitter Safety Setting

- 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 Figure 5

Figure 5
Snapchat World Map

- 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.

Results and Discussion

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.

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

Conclusions

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. A sense of security and online protection should depend on each user on making the web safer for everyone to use. The guideline will provide for a safer and secure social media, it would contribute a lot of help to the society that is shifting from manual task to online tasking their majority part of their lives. 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 Work

- 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.

Acknowledgements

Special thanks to Dr. Nelliud Torres Batista for his wisdom and support.

References

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

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

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

[4] A. Mosseri, "Working to Stop Misinformation and False News," Facebook Media, 07-Apr-2017. [Online]. Available: https://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news. [Accessed: 26-Apr-2019].

[5] J. Goodchild, "What Are the Seven Biggest Social Media Scams of 2018?," Security Intelligence, 24-Feb-2019. [Online]. Available: https://securityintelligence.com/what-are-the-seven-biggest-social-media-scams-of-2018/. [Accessed: 26-Apr-2019].

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

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