Social Media: The Unseen Risks of Cybercrimes

A Thesis Presented to the Faculty of Anna Maria College

Anna Maria College

In Partial Fulfillment of the Requirements of the Degree of

BACHELOR OF SCIENCE

in

CRIMINAL JUSTICE

by

Emily Ngo

December 4, 2020

Abstract

There is a rise in cybercrimes in recent years. More specifically, online harassment and cyberbullying are more prevalent and relevant especially with the rising popularity of social media. More and more individuals use social media for various purposes such as creating network connections to entertainment. This new territory provides questions and concerns about how users are affected as well as how they can protect themselves from offenders. Social media has provided specific crimes to predominate among its demographics. Certain information makes victims appear more attractive to their offenders. There are also instances, where one crime will interrelate with another. It raises questions about whether social media platforms have the duty to protect their users. Likewise, how can users protect themselves from being victims of both online harassment and cyberbullying? All data gathered is public knowledge originating from governmental agencies and reputable organizations with credible information. This research solely used U.S. data.

Social Media: The Unseen Risks of Cybercrimes

Social Media: The Unseen Risks of Cybercrimes

Chapter 1 – Introduction

The framework of social media is meant to connect others and engage users with each other. Individuals can now communicate with others, but businesses and organizations can also engage with consumers. News outlets as well can provide information to an audience. Social media has become a tool that people can use to engage with others quickly and effectively. The real-time element of social networking has made information accessible to nearly everyone (Wu, 2018, p. 2-3). The internet has an overwhelming amount of data collected from social media. Information, opinions, and frequent sharing with others are common occurrences seen over the internet. People use social media for different reasons. Some will use it to view activists' activities, others will look up information, but many will use it as a source of simple entertainment. News and public information are not typically things people think of associating with social media (Prieto Curiel, Cresci, Muntean, & Bishop, 2020, p. 2). However, statements of crime can be seen in one way or another.

A major challenge to dealing with social media networking is privacy and security on the accounts. There is a vast amount of data that is continuously flowing within social media platforms (Soomro & Hussain, 2019, p. 9). These digital platforms allow people to socialize with other like-minded individuals with common interests. There are ample opportunities for users to be able to work on collaborating projects, creating content, communicating and socializing with others, and gaming (Smith, Smith, & Blazka, 2017, p. 33-34). Currently, the largest social media networks are Facebook and Twitter.

Concerns over online anonymity, privacy, and security are valid. It is difficult to determine who exactly is the person online or how protected a person’s data is over the internet.

Social media has a unique ability to gather information as well as sharing it with others. Sites such as Twitter and Facebook allow users to communicate and share information. This can include images, videos, and mobile messages (Soomro & Hussain, 2019, p. 9). Social media users often forget, their privacy is at risk each time they are online. The reason is many individuals do not utilize their user settings on their social media accounts (Pavlik, 2017, p. 13). There are also dangers stemming from communicating with strangers online. Many people overshare details about their lives online with strangers and friends alike. For example, a user may post his or her plans of going on vacations for a certain amount of time. The individual explicitly said when he or she are leaving and the duration of the trip. With this information, a criminal can plan to successfully rob the user while he or she are away. By the time the victim returns, his or her property is already stolen.

With the increasing use of social media, cybercrime has become rampant. Standard cyber-attacks such as phishing, malware, and ransomware are indeed common. These basic attacks can damage a computer and at times a person's finance. However, with social media, the cybercriminals have finessed their methods of attack. The harm committed does not necessarily damage the user's computer, but rather effect the person in more physically and psychologically. Cybercriminals use the rapid connectivity of the internet to exploit the vulnerabilities of the network. Most people are unaware of this exploit, which makes bad individuals feel safe committing crimes in the digital era (Soomro & Hussain, 2019, p. 9). Criminals will use social media to plan their intended crime. They gather the information they need before executing the plan. The reason they can do this due to the quick response time of social media. They can commit crimes all in real-time (Soomro & Hussain, 2019, p. 10). Personal data is worth a lot in the underground economy. This information is easy to access considering many users overshare

details about their lives online. Due to this a cybercriminal can gather all the information and can sell up to $630 million yearly (Bir & Sodhi, 2020, p. 28-29). Victims will no longer have personal data. Frauds can occur, such as claiming social security benefits and opening new lines of credit with the victims' names.

Statement of Problem

A hot topic of online interaction is the harassment and bullying of an individual. This is a major problem due to the issue of having the potential of harming the victim. Persistent harassment and cyberbullying can impact the victim in detrimental ways. This is especially prevalent in online spaces (Pater, Kim, Mynatt, & Fiesler, 2016, p. 369). Accessing social media has become an incredibly easy task to do. There are multiples methods a person can now access the internet. Cybercriminals can easily gather information about the targeted victim. With the information they gathered, they can lure or contact a victim as frequently and severely, they want.

Online Harassment

Online harassment is not a manner to speak lightly of. Many people alone are affected by traditional harassment seen offline. For instance, repetitive inappropriate comments and unwanted touches are commonly seen in face to face situations. However, this can translate to an online space, which allows offenders to harass their victims in longer durations. Online harassment brings unique features that are not seen in traditional harassment. For instance, it is asynchronous in nature as well as portraying individuals to be anonymous users when interacting with others. It does not help that social media policy does not define actions to be considered harassment, which may allow others to continue behaving in such a way since no immediate consequence can be seen (Pater, Kim, Mynatt, & Fiesler, 2016, p. 369).

Cyberbullying

Cyberbullying is relatively a new phenomenon that researchers are still trying to figure out. Traditional bullying has always been an issue. Schools are still trying to mitigate bullying offline. Cyberbullying has provided a new method for victims to continuously be abused by not only known peers but strangers as well. What is more concerning is grown adults are viciously attacking unknown minors similar to how minors are attacking strangers. This poses an issue for both victims and their parents. There is a lack of credible resources to not only helped the victim but spread awareness of the problem to parents. It is difficult to mitigate cyberbullying, considering there is a large audience who seemingly attack a single figure who may not understand his or her rights or have means to protect themselves from the abuse (Espelage & Hong, 2016, p. 378).

Social Media as the Perfect Medium

The internet is a truly unique place where people can communicate with each other. Social media allows users to foster and grow their relationships with others. Likewise, it can help destroy and diminish the existing connection with others. When individuals engage in crimes such as online harassment and cyberbullying, there is a distinctive feature that allows offenders to feel comfortable committing malicious deeds. Anonymity is truly a major reason for many individuals allowing themselves to behave differently online. It hides the users' identity as well as not being able to face repercussions immediately. Likewise, mob mentality simply encourages other users to behave a specific way towards another individual (Lowry, Zhang, Wang, & Siponen, 2016, p. 17).

Online harassment and cyberbullying are truly relying on the anonymity factor that the internet brings. Often offenders may create fake or false accounts to actively abuse another

individual. Or they will act viciously to unknown strangers using either their account or a false one as well. It makes it difficult for offenders to be held accountable for their actions. Victims do have options to help lessen contact with those who are either harassing or bullying them. However, that does not necessarily stop those individuals from creating new accounts or asking others to continue the harsh treatment they were providing.

Background and Need

As of March 2019, internet users numbered 4,168,461,500. This essentially is 50.08% of the world population that is online. About 2.22 billion social media users worldwide are on the internet. This accounts for about 31% of internet users being on social media. The numbers are expected to reach over 3 billion by 2021 (Soomro & Hussain, 2019, p. 9). With nearly a third of the world population on social media, it is expected that there will be some bad actors on it. Cybercriminals can do a range of malicious deeds. It can range from something minor such as spreading hate comments on someone to trying to attack a nation's government. These criminals have various ways of obtaining information from their victims. Most often it is social engineering methods. Cybercriminals intentionally use fear and urgency to make their intended target panic. By doing so, the victim will not think rationally or question the cybercriminal about the situation (Soomro & Hussain, 2019, p. 10).

Online Harassment

Online harassment can appear in many forms. This can include hate speech, cyberstalking, sexual harassment, and to an extent cyberbullying. Unfortunately, these incidents can foster victims' obtain self-destructive behaviors and tendencies such as having an eating disorder, self-harming oneself, and at times committing suicide (Pater, Kim, Mynatt, & Fiesler, 2016, p. 369). It does not help either that social media platforms can provide offenders a

medium to harassed other users. All platforms do have policies that can mitigate the issue. Yet, there is no real concept defined, which makes it easier for the victim to stop the abuse they are facing. Perpetrators specifically target other users based on certain characteristics or criteria an individual may possessed. It does not help that attacking people based on racial appearance or culture is one of the more common ways an offender targets or abuse the victims. It is not uncommon for foul language or slurs to be used as well as offenders creating posts specific targeting aspects of the victim on their account (Silva, Mondal, Correa, Benevenuto, & Qcri, 2016, p. 3). There is a pattern for online harassment. If the victim was previously or is currently in a relationship, online harassment is more likely to occur. The reason is intimate partners who display signs of intense jealousy or upset with the victim will engage in harassing behavior online. Victims also have a high chance of facing online harassment by someone they were once or currently intimate with. Social media allows people to have access to one another in the most accessible way. Electronic devices, apps, and internet access will simply increase the amount of abuse or harassment the individual will face (Wick et al., 2017, p. 25).

Cyberbullying

There is a connection between social media and cyberbullying. Social media is different compared to traditional websites. These social platforms allow users to actively and knowingly share private information about themselves to the online realm. Young users do not necessarily understand their actions and how easy it is for others to view the information they publicly share. In terms of cyberbullying, bullies can use information from their targets and deliberately use it against their victims. It also helps foster traditional bullying if the victims know their bullies. It can lead to physical confrontations and altercations seen in both the public and school environments (Garett, Lord, & Young, 2016, p. 1). It does not help that there is a median

prevalence of 23% of cyberbullying reported. The effects it has on the victims are devastating. The abuse a victim faced can easily be instant, spread to a wider audience, and leave lasting effects that can result in permanent results such as suicide. It is even worse if the victim does not necessarily have means to support or defend themselves during these troubling times (Hamm et al., 2015, p. 771). However, resources are becoming more relatively available to all who need them. Movement within the government has occurred as well as organizations spreading awareness to both parents and victims about this situation. Still, more protective and intervention methods are needed to ensure the issue is dealt with properly. Justice needs to be served appropriately (Espelage & Hong, 2016, p. 375).

Social Media as the Perfect Medium

The internet allows individuals a wide range of activities to do online. Social media is simply a byproduct of an activity users can participate in as a source of entertainment. Social media crimes are unique compared to traditional crimes. First, there are social media-assisted crimes, meaning these crimes will be committed even if the social media element is removed. The criminal will find another alternative to commit the act. Second, there are social media-enabled crimes. These are more traditional crimes already regulated in criminal law. However, if the social media element is removed, these crimes will be reduced. Lastly, there are social media crimes dependent on social media platforms. These crimes are do not exist within the scope of the criminal justice system, nor does the system knows how to interpret it (Bir & Sodhi, 2020, p. 33-34). Anonymity is the major factor of why criminals choose to conduct their crimes through social media. Social media allows individuals to remain anonymous through various means. For instance, false identities, pseudonyms, and throwaway accounts are constantly used. Different online tools can help keep this charade going. Browser extensions are one method used to hide a

person's identity from social media platforms (Lowry, Zhang, Wang, & Siponen, 2016, p. 17-18). Likewise, with the open channels of communication that social media has provided, social engineering is taken to the next level. Social engineers use the platform to choose and gather information on a target. Victims can be lured into providing information that they would not necessarily provide if they were not manipulated or persuaded to do so (Wilcox & Bhattacharya, 2020, p. 2).

There are common themes shown with the two cybercrimes previously mentioned. Abuse, variations of methods, social media used as a vector, and last effects on victims are seen. Online harassment and cyberbullying are seen to be new types of crimes. Despite being modeled on traditional crimes, they are a modified version that utilizes the internet and electronic devices. Often these crimes can also be compatible with their traditional counterparts, and victims are left worrying about their well-being since they have no gateway to escape their offenders. Perpetrators are becoming more tech-savvy as well as displaying vicious behaviors to both strangers and acquaintances alike. There is a consensus of prevention and intervention being needed and enforced more often.

Purpose of the Study

The purpose of the study is to demonstrate that social media has increased cybercrime. The crime itself is more complex. There are often factors that contribute to it. It can range from what the social and economic features are to what motivates an individual. However, with the rise of social media, it is difficult to determine what is a crime. Also some individuals believed that they are “joking” or “trying to be funny.” They are unaware of the effect their actions have on an individual nor do they understand what they are doing is a crime.

Technology is continuously advancing. The internet is simply a byproduct of what

science has created. The phenomena of cybercrime is still a relatively new field. And with the rise of social media, the user base seems to grow. The demographic of the users seems to be diverse and younger users are more reliant on social media and do not realize the dangers of it.

This study is mainly conducting researching. It will examine two specific cybercrimes committed on social media. Graphs and statistics are used to demonstrate the severity of the cybercrime seen on social media. All this information comes from credible sources that have been thoroughly vetted and used by professionals. I expect there has been an increase in crimes due to increase usage of social media. People will often allow their emotions such as jealousy and hatred to commit crimes such as cyberbullying and online harassment. If these crimes are done online, they still have a real-life effect and can impact the victim heavily. I hypothesize that individuals who overshare on social media are more likely to become victims of cybercrimes. This is due to the individuals posting information such as their likes, location, and life experiences to everyone on social media, without censoring themselves. This allows cybercriminals to use the information they gather to do whatever they please.

Research Questions

- What crimes can be committed?
- What type of information does a person post that makes them an attractive victim?
- How these crimes affect others?
- Do social media platforms have a duty to protect users?
- What can social media users do to protect themselves?

Significance to Field

This is significant in the cybersecurity field since social media is gaining popularity over the years. People often overshare personal information unknowingly and do not think of the

consequences. Cybercriminals can use this information to do various crimes such as locating the victim in real life to gaining access to their online accounts. Also, this goes in hand with the idea that people will use the anonymity factor of the internet to remain anonymous. By doing this they believe that they will not face any repercussions, nor do they believe their harmful and hateful comments will personally affect them in real life.

Definitions

- Cybercriminal is a person who does criminal activity through the internet or computer devices.
- Cybercrime is a criminal activity done using the internet or computer devices.
- Cyberbullying is using electrical communications or devices to harass, bully, harm, or intimidate an individual who is unable to defend himself or herself. These acts are deliberate and repetitive. Typically, both parties and the victim are minors.
- Online Harassment is using electrical communication or device to harass, bully, harm, or intimidate an individual who is unable to defend themselves. These acts are deliberate and repetitive. Typically, both parties are over the age of eighteen.
- Social Engineering is a method used to manipulate a person into revealing confidential or personal information for malicious purposes.

Limitations

The limitation of the study is all data gathered is limited to only the U.S. region and citizens. Public data is gathered from government departments and credible organizations. Most reports found are either conducted annually or gathered for a specific period. The data gathered reflect only what has been reported to the various agencies and organizations. There was also time constriction on the paper, which resulted in a limited time of gathering information. Proper

research could not be conducted due to COVID-19.

Ethical Considerations

This project consists of researching and analyzing the connection between social media and cybercrimes. No ethical consideration is required for this project. No human participants were needed in my research.

Summary

The new era of technology holds uncertainty for all. New features and online activities were seen on the internet brings forth unexpected problems and unintended consequences.

Chapter 2 – Review of Literature

Society has always dealt with criminal activity within its population. Theft, harassment, and fraud are common types of crime. However, as society begins to evolve so does crime. New tools and methods are used, which in return improves combat ability and justice against them. In today's era, traditional crimes are making appearances within the digital realm. What is most prevalent is online harassment and cyberbullying. Social media has provided offenders a medium from which they can act vile towards others online.

In this literature review, I will be examining the keys components seen within my topic. The first component is online harassment. I will be discussing how online harassment is prevalent within social media and how users are affected by it. From the literature, it is seen online harassment is a major issue for various users. This is due to specific individuals being target by both strangers and known people who are the perpetrators. The second component is cyberbullying. There is a connection between social media and cyberbullying. Cyberbullying leaves an impact on victims, which results in a call for action to mitigate this issue. It is seen that cyberbullying is an evolving problem stemming from traditional bullying. With the cyber aspect, the lasting effects can be more devastating than traditional bullying alone. Lastly, social media is the perfect medium for cybercrimes. There are unique aspects that make cybercrimes truly different than traditional crimes. Social media is simply used as a medium due to the advantages it brings. Offenders have their reasoning for committing online harassment or cyberbullying.

Online Harassment

Online harassment is becoming more common in the social networking environment. Pater and her fellow researchers (2016) compared social media platforms' policies regarding

online harassment. Social media platforms have different policies about online harassment, despite it being in the same digital environment. Their study is meant to help provide a better understanding of various social media platforms and appropriate ways to intervene whenever online harassment or similar instances occurs (Pater, Kim, Mynatt, & Fiesler, 2016, p. 369). Fifteen of the most popular social media platforms were analyzed. A total number of fifty-six documents were examined, including formal and informal policies such as privacy policies and community guidelines, respectively. Two researchers independently coded randomized samples of documents. Afterward, the two discussed general themes found before expanding the coding of words. After analyzing social media's policies, it was determined the majority of the platforms did not define what is harassment. Meanwhile, Instagram and Twitter were the two platforms for specific behaviors and activities that count as harassment. Overall, 37.5% of all documents had a form of harassment or derivation of it to appear in all policy documents. Strangely enough, all platforms except for Vine and VK directly mentioned harassment. Twenty-one out of the fifty-six documents explicitly mentioned harassment despite never defining it. It is found that six platforms mentioned harassment informal policies while two platforms mentioned it in informal policies. Yet only five platforms mentioned harassment in both formal and informal policies (Pater, Kim, Mynatt, & Fiesler, 2016, p. 371-372).

Online harassment can come in many different forms. Hate speech is commonly seen in cases of online harassment. Silva and his team (2016) realized the challenges social media has in balancing freedom of speech and defending human dignity. Hate speech is a byproduct of online harassment that is commonly seen on social platforms. Their research was created to have a better understanding of the variation of online hate speech. The team gathered their data from Whisper and Twitter, two popular social media sites. To measure, definitions were created to

help define terms and meet specific criteria. Hate speech is defined as "any offense motivated, in whole or in a part, by the offender's bias against an aspect of a group of people" (Silva, Mondal, Correa, Benevenuto, & Qcri, 2016, p. 1-2). With this, the researchers used sentence structure to help determine if a post contains hate speech, though there were times it did not identify existing hate speech. As a result, both platforms have similar hate targets. Common categories found were race, behavior, physical characteristics, sexual orientation, class, genders, ethnicity, disability, religion, and other personal characteristics. For Twitter, 48.73% of posts target people by race; meanwhile Whisper had 35.81% of behavior characteristics targeted (Silva, Mondal, Correa, Benevenuto, & Qcri, 2016, p. 3-4).

Wick and his colleagues (2017) tried to determine patterns and perceptions of online harassment among college students within the U.S, most notably those who are previously or currently in intimate relationships. Typically, online harassment involves threatening, insulting, harassing, or harming individuals through electric technological methods or devices. In this study, Wick and his colleagues (2017) examine the effects of online behavior and determined the risks are for online harassment (Wick et al., 2017, p. 29). Two hundred ninety-nine undergraduates' students participated in an anonymous online survey. Multiple scales were used to measure the responses. Five different aspects were considered such as cyber harassment-victimization, cyber harassment perpetration, risk propensity, online exposure, and online disclosure (Wick et al., 2017, p. 29-30). The results found risk propensity differs between genders. Male college students are shown to have greater levels of risk propensity compared to female college students. About less than 21% of participants never experienced any online harassment while 18% reported never committing any forms of online harassment (Wick et al., 2017, p. 31).

Social media needs to adopt stricter policies into defining what behavior is seen to be harassment. Likewise, a clearer definition of what harassment is and how offenders will be punished if they continually harass another user. Far too many individuals are quite comfortable in posting harassment materials such as hate speech on their accounts publicly. It is interesting to note though that victims are likely to know their offenders especially if they were once in an intimate relationship with them.

Cyberbullying

Cyberbullying is a major public concern that can lead to devastating effects on its victims. Garett, Lord, and Young (2016) are determined to find the frequency of cyberbullying by evaluating a previously published paper. Considering cyberbully to be relatively new within the field, they determined it was best to conduct a systematic search on PubMed and PsycINFO. They mainly searched terms consisting of "cyberbullying" and deviations of social media and specific platforms. As result, 307 papers were found, 98 stemming from PubMed and 209 appearing in PsycINFO. Four criteria were applied to ensure the papers applied to cyberbullying. This narrowed the number of papers to be analyzed to 79 instead of 307. While analyzing the data, papers were placed in categories based on author and year publications, same characteristics, study characteristics, cyberbullying factors, and frequency and concept of cyberbullying. The papers were broken down, even more, to focus on either victim, bullies, and bystanders and were analyzed through a regression model. This helped eliminated papers down to 22. The results found shown an increase in cyberbullying with a three-year review period. It is generally agreed that cyberbullying indeed affects the younger generations. 14 (63.6%) had samples of middle and high schoolers, 9 (40.9%) of college students, and 3 (13.6%) of primary school students. Facebook (45.4%) and MySpace (13.6%) were the most common platforms to

be used. Interestingly enough, the paper had acknowledged that there is still a lack of agreement on knowing the instruments used were accurate. It was undetermined if what they measured was either cyberbully, electronic bullying, or internet harassment (Garett, Lord, & Young, 2016, p. 2-4).

Hamm et al (2015) believed social media has a high impact on children and adolescents. One of the major harmful potentials has the consequences stemming from cyberbullying. A scope method was used to examine social media as well as to create a chart that helps illustrate evidence they found. Originally, the team has used databased entering keywords into finding the material needed. 10,289 records were identified, but after removing all duplicate records 8173 records remained. 8173 studies were screened yet 36 studies were able to meet the criteria Hamm and her colleagues set forth. To lower the numbered of studies examined, the group chooses to focus on full-text articles. This lowered the total to 662 eligible studies to be reviewed. Afterward, only 36 studies met the criteria the researchers applied. About 21 (58.3%) of the study took place in the U.S. About 24 (66.7%) had sampled middle and high schoolers. The average participants within the study populations were females of 55.8% and males of 44.1%. The results demonstrated 91% of cyberbullying occurred due to relationship issues. The study includes break-ups, envy, intolerance, and ganging upon the individual to be part of the relationship. Also two studies have stated gossip and rumors to be circling romantic relationships. Girls often received messages about their appearances or popularity. They would often be excluded or isolated by others online. Meanwhile, boys received homophobic messages or harmful comments about their physical attributes or abilities (Hamm et al., 2015, p. 772).

It is no surprise the public is concerned with bullying. Cyberbullying is simply a byproduct occurring through electronic devices. Espelage and Hong (2016) hope to examine the

prevention and intervention of this phenomenon. The two have examined various articles and resources regarding the evolution of cyberbullying and any prevention efforts shown in North America. Other real cases such as the deaths of Megan Meiers, Phoebe Prince, and Amanda Todd were also examined, due to these individuals being victims of cyberbullying. Both researchers have found that many scholars believe prevention and intervention is the key to mitigating cyberbullying. However, there is no agreement on how to prevent or even address the issue. Rather a common strategy is seen through various resources that victims and parents can use. That is providing easily accessible resources regarding cyberbullying and how to avoid being a victim. Various sites and fact sheets are typically shown as resources. About seventeen cyberbullying prevention sites were examined. Only fourteen were designed for parents, seven were meant for young children between ages of six and ten, eight were for tweens of the age of eleven and twelve, and lastly, eleven were for adolescents of thirteen and eighteen years. Nine were addressed to school officials while six were meant for law enforcement. Surprisingly six sites were centered around a commercial product while only ten sites included evidence from published research. It is seen that prevention programs are targeting parents with information. Often, online resources seemed to be promoting products that are being sold from an organization with little evidence to support it. It is shown those sites prove to be risks since the information they are promoting are false (Espelage & Hong, 2016, p. 375-376).

Bullying is always issue schools continually face. However, with social media cyberbullying continues the cycle online. Victims have specific attributes of themselves that offenders like to target. With this growing problem, it is only natural for prevention and intervention efforts to emerge, but more issues emerge instead. There is a lack of credible resources for victims to use if they are facing cyberbullying.

Social Media as the Perfect Medium

Social media is one of the most interactive platforms online. Millions of users worldwide are constantly engaging with each other. Bir and Sodhi (2020) demonstrate how social media is integrated into our daily lives. The two researchers analyzed the specific applications, their marketing tactics, and customer relationships marketing. All data they gathered includes the various ways a user will interact with social media platforms and legislation surrounding it. Through various publications, the study showed an increase in trends surrounding social sites. They gathered through a Global Digital Report, that worldwide internet users have increased by 9.1% from 2019 ranging to be about 4.388 billion. Meanwhile, social media users increased by 9.1% globally, making it to be about 3.484 billion (Bir & Sodhi, 2020, p. 7). With this, Bir and Sodhi noticed an increase in cybercrimes on social media. They theorized cybercrimes have elements to create performance crimes that are uniquely seen on social media. Performance crime is categorized into two types. One is informed consent. This performance crime consists of individuals performing a crime and being aware of it. Typically, the individual will record it or film it himself or herself and have the intention of distributing the video later. The offender is considered an actor and will behave as such in front of the camera. The second type of performance crime is when the individuals are recorded without being informed nor are willing to be part of the crime. They typically have no knowledge that the event is being recorded (Bir & Sodhi, 2020, p. 10).

There is a strange phenomenon of individuals harassing or bullying others online. Lowry and his colleagues (2016) examined 135 articles regarding cyberbullying to have a better understanding of this concept. The use of social structures and social learning models helped measure and fill in gaps that the articles they reviewed missed. Overall, the team believed

anonymity can explain criminal behavior through the theory of online disinhibition. This theory leans towards the idea of individuals exhibiting the same general negative characteristics online correlates to the high rate of cybercrimes. For instance, a person may witness a group of users using the same language towards a single figure, which makes the person believe the group behavior is appropriate. The anonymous communication with another also reduces social accountability of oneself. This suggests people will engage much more negatively and aggressively due to believing there is a lack of accountability on their end. The digital space makes users feel as if they can perform any actions that they would not typically do offline (Lowry, Zhang, Wang, & Siponen, 2016, p. 18). Lowry and colleagues also found anonymity lead to deindividuation. This means a person will lose his or her sense of individuality and personal responsibility for his or her actions. They have found anonymity to be the major cause of deindividuation. This is prevalent in a large group. If an individual found themselves in this situation, he or she will lose self-awareness and follow the actions of the group they are in (Lowry, Zhang, Wang, & Siponen, 2016, p. 19).

Social media has provided communication channels to all users. With this accessibility of being able to communicate, users are more inclined to interact with each other. Wilcox and Bhattacharya see social engineering as a method that allows cybercrimes to be rather prevalent. Internet users are more sustainable than outside influence. The two authors have studied global trends about the online environment and cybersecurity concerns. They analyzed different social media and information security scenarios in various regions to obtain the data. They also have conducted a study using a descriptive survey to measure individuals' experiences of social engineering through social media in both public and private organizations. However, this study has taken place in Australia, not in the U.S. The survey included closed and opened questions

about people, process, and technology used to gather data for social media management, awareness of social engineering, and technical threats mitigation measures (Wilcox & Bhattacharya, 2020, p. 4). The two researchers have introduced a cycle that social engineering follows to measure their findings. There are four phases that each social engineer engaged in. The first step of the cycle is factfinding where the individual will gather information about the target. In this phase, the perpetrator will foster a relationship with the target or someone close to him or her. The second phase is entrustment. The perpetrator will place himself or herself in a position of trust. The third phase is manipulation. The target is blinded by the "trust" he or she hold to the perpetrator. They are manipulated to provide information unknowingly to the perpetrator or commit actions for them. The last phase is the execution. This completes the cycle due to the target completing the tasks requested by the perpetrator (Wilcox & Bhattacharya, 2020, p. 2). There is about 70% of management personnel have guides or promoting employees to use social media in a specific way. These guides dictate a separation between both personal and professional usage of social media from the employee. However, many employees are confused about the distinction between the two accounts (Wilcox & Bhattacharya, 2020, p. 5).

Social media is a global activity that nearly the whole world is participating in. This digital landscape allows new ideas and techniques to emerge, including crime. Crime is not always consensual nor many purposeful wishes to be part of. Perpetrators of cybercrimes usually have their reasoning to commit the bad deed. However, in cases of online harassment or cyberbullying, mob mentality plays a role in how a user interacts with another. Communication between users is not always clear, and room for confusion and misunderstanding can occur.

Summary

Overall, human connection drives users to communicate with each other. However, intentions for contacting another may not be as pure or friendly as many would like to think. Without the proper definition of ill-mannered or hateful actions such as harassment, it makes it difficult for social media users to take action in cases such as online harassment and cyberbullying occur. Even more so, with the rise of new social media users, an increase in cybercrimes is bound to happen. Social media crimes have unique aspects that make them truly different compared to traditional crimes. In my study, I'm demonstrating how social media influence cybercrimes and the impact it has on not only the victim but on the public as well

Chapter 3 – Methods

As a society, many of us are becoming more and more connected online. Technology is slowing enhancing how users can communicate with others. Information such as present location, daily activities, thoughts, and other personal details are posted online. Many users feel comfortable sharing these aspects of their life, however, doing so comes with a cost. Cybercriminals may use the information found to conduct a crime. The rapid pace of internet connection allows bad actors to view, plan, and commit crimes all in real-time. Many are unaware of their vulnerabilities and often become victims themselves. Social media directly influence cybercrime on the platform. Victims are severely impacted by what transpired between themselves and the other individuals interacting with them.

What type of information does a person post that makes them an attractive victim? What crimes can be committed? How these crimes affect others? Do social media platforms have a duty to protect users? What can social media users do to protect themselves? These are the questions that this paper will attempt to answer.

For this research, public data is collected from reputable and creditable organizations. For instance, the FBI's Internet Crime Complaint Center (IC3) and Pew Research Center are analyzed. Many of these organizations released annual reports to the public. These reports center around specific aspects seen within the cybersecurity field or cybercrimes trends. Information released includes statistical data, crime types, and other key features important for the field. All this data will be used to create an original analysis of social media and cybercrimes.

Setting

Considering my thesis is reliant on more public data to create an original analysis, no real

setting has taken place. All my material was gathered online through the Anna Maria College database, Google Scholar, the Bureau of Justice Statistics, and the Google search engine. No physical residence was needed for my research. However, my thesis solely focused on cybercrimes that occurred in the U.S.

Participants

My paper does not use human participants at all. However, it does use public data from various sources. Many of my data stems from Statista, a digital data platform used by various businesses and industries worldwide; Pew Research Center, an organization that provides credible data and information on various topics to the public; The Internet Crime Center, a division seen within the FBI, that specializes in all cyber-related crimes and lastly, the National Center for Education Statistics (NCES), a federal organization within the U.S. Department of Education, which provides statistical data nationally. These data all focused solely on U.S. citizens.

Intervention

In my research, I will be examining a connection between cybercrimes and the victims. By analyzing data about online harassment and cyberbullying, I can see how these cybercrimes influence or affect the victims. The impact the cybercrime had on the victim will determine the severity of the relationship between the two variables.

Materials

The material used is solely data seen from credible organizations mentioned before. Data about online harassment is extracted from Statista, Pew Research Center, and the IC3. It goes more in-depth about users' experience of online harassment, attitudes towards it, and the effects it has on the victim. Cyberbullying data is also extracted by the Pew Research Center and the

NCES. I would also be observing users' social media habits such as account activity, privatizations of accounts, protective actions on social media, and concerns. However, it will be focused more on Facebook users. Total cost loss stemming from social media crime are also being used. This type of data is found within IC3's report. Social media users have different attitudes about social media and cybercrimes connected to it. Each user faced uniquely different experiences stemming from online harassment and cyberbullying as well as having different styles of handling the situation. Social media habits vary, and some may change after being affected by a specific event.

Measurement Instruments

The measurement instruments for this research consists of public data from various organizations. The most common way for the information to be obtained is through surveys. Each survey consists of participants from the U.S. over the age of eighteen. Their answers were recorded. For instance, Statista's surveys were conducted through online surveys bringing in a large number of participants ranging from 800 to 1200, depending on the topic. Meanwhile Pew Research Center gathered data through random-digit-dial surveys as well as online surveys. NCES gathers its data through their department as well as the Bureau of Justice Statistics. Online harassment data details information on what type of harassment occurred, what attackers typically targeted for, how harassment affects users, and who may be the offender. Cyberbullying data centers more around frequency, type of cyberbullying, the environment it occurs, and level of schooling. Social media habits were surveyed as well. Data about how private is a person's account, protection actions users committed, and concerns over the platform will be analyzed. The numbered amount of the total cost loss have been gathered as well to support the effects cybercrimes had. All these surveys and reports measured the specific topic as

best as they can with the responses they received. There are high volumes of responses for each survey. With this amount, there is a small margin of error to occur.

Procedure: Qualitative Study

The data was collected solely online. Various databases and online searching for data occur for about five weeks. Databases from Anna Maria College, Google Scholar, and the Bureau of Justice Statistics were used to find reports and information about online harassment and cyberbullying. Google searches were also done to find more data from reputable organizations such as Statista and Pew Research Center. Time was dedicated to analyzing and separate data into different categories. One category dealt with online harassment, one for cyberbullying, total cost loss of cybercrimes, and protective measurements on social media. All this data is analyzed to find a connection between social media and cybercrimes and how extensive this relationship is. However, much of the data collected refers to users experience on Facebook.

Data Analysis

The data has been collected and categorized to fit the specific key aspect the paper shown. As mentioned before, the four categories were created to help find the relationship between social media and cybercrimes. Specific surveys and annual reports were chosen to help answer the researched questions. The statistical data shown demonstrated connections between social media and the surging trend of online harassment and cyberbullying. Even though many users are becoming more aware of this phenomenon, attitudes differ about these crimes. The data diverge into people’s feelings about social media platforms' involvement in protecting users as well as who is responsible for it. There is an interesting correlation of attitudes differing between genders and age groups. All data have been compared to see how this connection can

be made. The data will be presented in a narrative format. Graphs will be used to help illustrate the statistical data found.

Conclusion

By having a variety of data, a clearer connection between cybercrimes and victims can be more accurately shown. Different habits, harassing or bullying methods, frequency, and duration of the crime will vary between each victim. All the public data gathered can help solve the questions that were previously mentioned.

Chapter 4 – Results and Findings

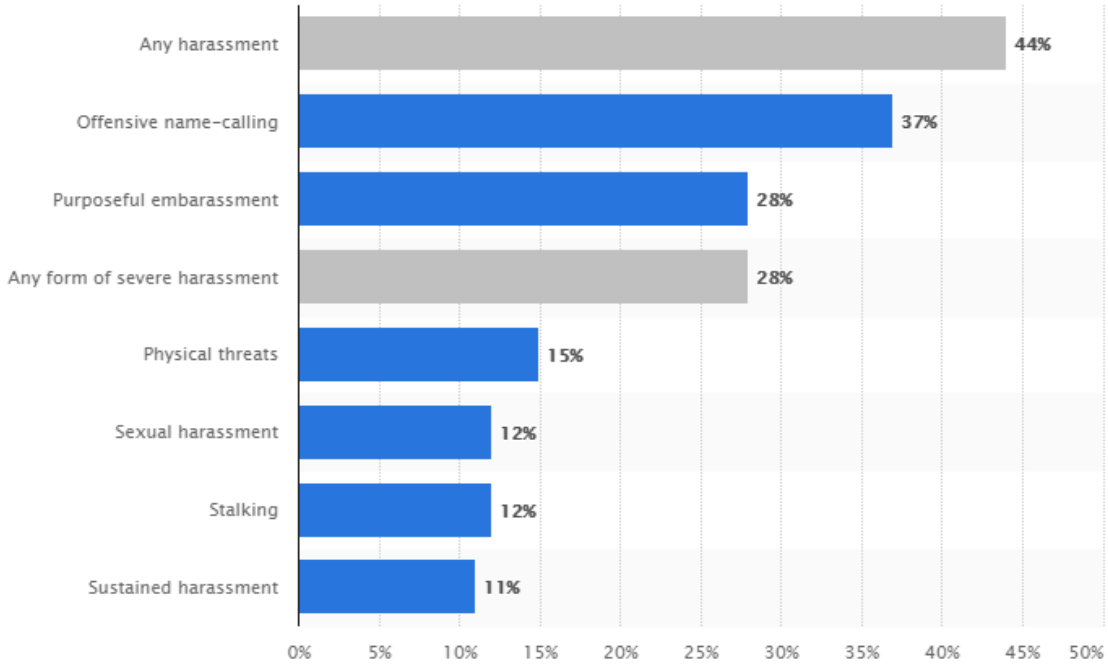
Social media provides a new element within the scene of cybercrimes. Users now have the resources to not only research and communicate with people they know but with strangers as well. The online community is not focused on one region in the world, but globally instead. Crimes such as online harassment and cyberbullying can reach nearly anyone. Social media users are mostly affected by this phenomenon, however, how they handle this can differ.

Online Harassment

Online harassment is not far off from traditional harassment. The only difference is the environment where it takes place. This crime heavily involves other malicious acts such as cyberstalking, leaving disturbing or threatening messages, hate speech comments, etc. As shown below Statista reported overall 44% of internet users have faced a form of harassment while 28% of internet users faced a form of severe harassment. The graph breaks down even more into the type of harassment a user experienced. Within any type of harassment category, offensive name-calling and purposeful embarrassment are the two common styles of harassment. Meanwhile in the severe harassment category physical threats, stalking, and sustained harassment was more prevalent. Considering there are nearly 2,000 responses, it is safe to say about four out of ten American users will be harassed online.

Table 1

Share of adult internet users in the United States who have personally experienced online harassment as of January 2020



To examine this further, it is better to look at what characteristics or reasoning someone used to harass another. There are different characteristics or features offenders will target. The more common characteristics are personal or physical attributes such as personal appearance, ethnicity, gender, and political views. Pew Research Center created a spectrum of how severe online harassment is shown in Table 2. It is shown users who were harassed were affected differently depending on the severity of the harassment. Mental and emotional stress was the major effect that many individuals felt. Those who did not experience severe behavior were about 20%; meanwhile those who faced severe behaviors were about 34% experienced mental and emotional stress.

Table 2

Those who have faced severe forms of online harassment

Copyright 2017 by Pew Research Center

It is shown that younger adults are more likely to experience severe forms of online harassment. About 67% of internet users between the age of 18 – 29 experienced online harassment. This is twice the number of what users within the 30+ age group will face. This can be due to younger individuals being more likely to be online compared to their older counterparts as well as having more social media accounts. Overall, of those who experienced online harassment, the majority stated it to take place on social media. A survey was conducted through the Pew Research Center and demonstrated that 58% of the harassment took place on social media platforms. It breaks it up even further to describe an individual experienced of harassment on one platform by 82% while others were harassed on multiple platforms by 18%. However, it is interesting to note that strangers and individuals with fake personas are more likely to harass another user, when comparing it to harassers knowing their victim. About 34% were strangers while 31% are individuals were real identity of the offenders were unknown. Meanwhile, 5% of offenders were a coworker of the victim.

Cyberbullying

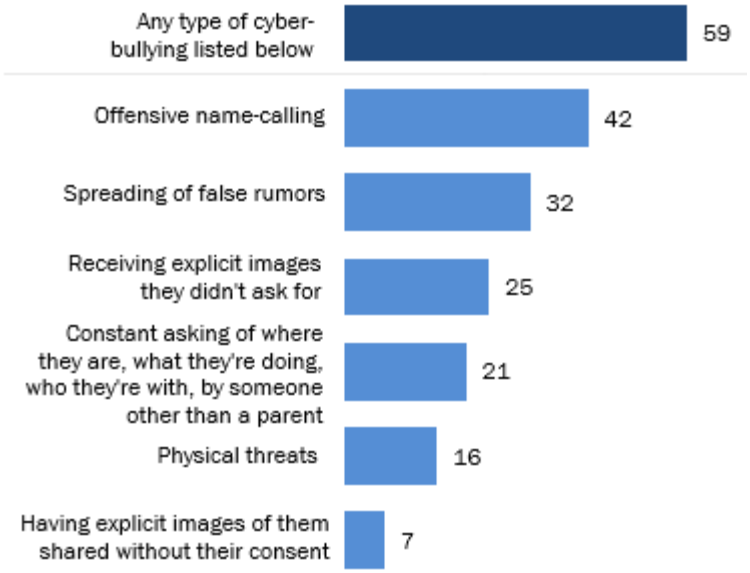
The NCES gathered intel regarding cyberbullying within the U.S. Cyberbullying is becoming a growing problem due to its compatibility with traditional bullying. Many considered

cyberbullying to fall in the same category as online harassment. However, the difference between the two is the age of the victims. Cyberbullying mainly pertains to victims who are minors while online harassment does not. During the 2017-18 school year, cyberbullying frequently occurred at least once a week. The NCES determined cyberbullying effects all public schools nearly 15% of the time. However, it is the highest in both middle schools and high school with 33.1% and 30.2% respectively. Meanwhile, it occurred the lowest in primary school at 4.5%. If the school system is combined, 20.2% of cyberbully has been reported. This makes sense considering middle schoolers and high schoolers are more likely to have electronic devices such as cell phones to connect to social media. Also, nearly all social media platforms required the user to be at least 13 years old before creating an account.

Pew Research Center found that 59% of U.S. teens have experienced cyberbullying. In Table 3, it demonstrated the various forms of bullying and harassment that many teens experience. The most common attack is offensive name-calling at 42% and having false rumors spread at 32%. Meanwhile having explicit images shared without consent is shown to be least by 7%. Many young users also reported that they faced combinations of attacks. Any bullying shown online has the potential of transferring into the physical school environment and continue the cycle.

Table 3

A majority of teens have been the target of cyberbullying



There is a difference between the genders of the victims. Females are more likely to become victims than their male counterparts. However, it is important to note there are some instances where there are barely differences between the two genders. For instance, 59% of males experienced cyberbullying while 60% of females experienced the same. Name-calling and physical threats are two methods where both genders practically have a percentage of 42% and 16% respectively. However, females experienced false rumors about them at 39%, unsolicited explicit images receive at 29%, persistence of unnecessary questions by 23%, and their own explicit images of them shared without consent by 9%. Males experienced the same treatment at a lower rate. The spread of false rumors affected 26%, unsolicited explicit images receive 20%, persistence of unnecessary questions 18%, and their own explicit images shared without consent 5%. It is important to note multiple victims may face a combination of cyberbullying attacks.

Total Cost Loss

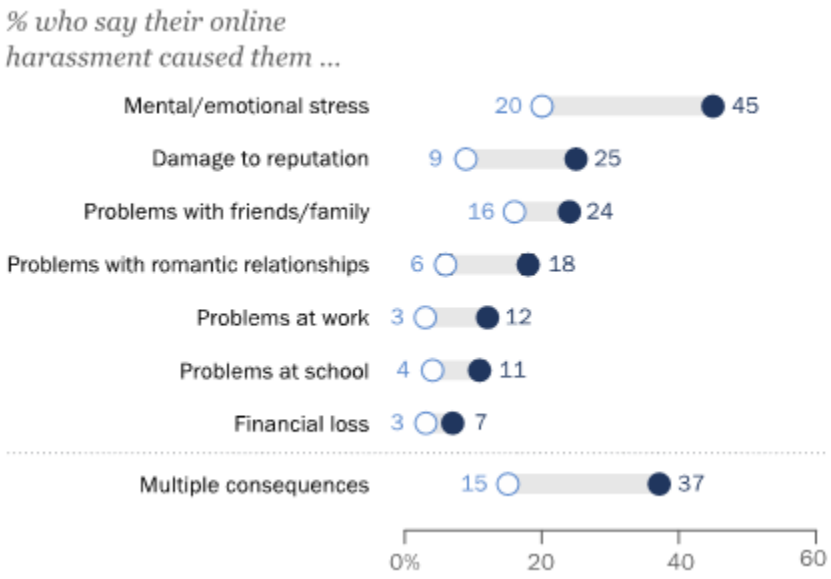
Cybercrimes can leave a lasting impact on not only the victims but on the economy as well. This style of crimes can involve a simple fraud to being a threat to national security such

as terrorism. Social media is simply more of a vector used to help conduct crimes. The IC3 reported $3.5 billion was the total cost lost in the year 2019, which average the daily complaints to be over 1,200. Social media crimes generated $78,775,408 in the past year alone with about 29,093 known cases. For crimes such as harassment and threat of violence, 15,502 victims were known, generating $19,866,654 total cost lost.

Online harassment heavily affected not only victims but bystanders as well. Victims from this crime potentially experience mental and emotional stress to financial loss. In some cases, multiple consequences can be seen. Table 4 portrays the effects online harassment has caused, both involving non-severe and severe behavior. As stated, before mental and emotional stress was the major effect of harassment while the financial loss was least to occur. Strangely enough, it is reported that out of the participants reporting harassment, 61% chose to ignore the harassment incident while 39% chose to respond. Of those who choose to take action 50% confronted the person online while 49% unfriended or blocked the person. Harassment incidents are reported to either law enforcement or employers and schools 5% of the time. Bystanders who witnessed the situation were influenced by the event. About 28% adjusted their privacy settings on accounts and 27% chose not to post something online. Also 16% changed their online profiles, and 13% stopped using the platform altogether. 47% of users reported doing a combination of these tactics.

Table 4

Who says their online harassment caused them?



Regarding cyberbullying, it is known that bullying continues offline as well. About 21% of middle schools reported the school environment being affected by cyberbullying while 18% of high schools reported the same. Often cyberbullying has the same effect seen in online harassment. Luckily, schools have implemented resources for both victims and their parents to use if their child is being cyberbullied.

Protective Measurements

One-way social media users can protect themselves on social medias by controlling their privacy settings. Luckily, it seems a good number of users do privatize their social media accounts. Statista shows the majority of users between the age group of 30-44 years, 45-54 years, and 55-64 years to privatizing all their accounts by 52%, 48%, and 45% respectively. Meanwhile, those in 18-29 years group and 65+ have the least percentage of 40% and 38%. This demonstrates that it is more likely most young adults are building a brand for themselves while elderly individuals are unaware of these features. However, with the rise of cybercrime awareness, internet users are taking a precaution on all online interactions. It is shown 45% of

individuals will avoid opening emails from unknown sources and 41% will disclose less personal information. Strangely enough, 11% of individuals choose to close social media accounts and 8% choose the internet less often. Many social media platforms do have policies used to ensure all members are comfortable and safe while interacting with their platforms. They do incorporate features such as unfriending, blocking a user, and reporting any issue to the platform. However, many feel that online platforms need to do more to combat online harassment and cyberbullying of users.

Conclusion

Unfortunately, online harassment and cyberbullying is a growing problem. However, many users are being aware of the harmful potential social media brings. People are taking precautions while they are online to avoid being a victim themselves.

Chapter 5 – Discussion

The internet landscape is becoming more complex and relevant as time goes by. The digital world provides an avenue for all users to connect with one and another. Social media is an activity that many do participate in and becoming necessity to have, whether it is for personal or professional reasons. This study was to determine the impact social media crime and how social media influence it. The two crimes I mainly focused on is online harassment and cyberbullying. Through the data collection, it is shown that social media do enable cybercrimes from the statistical studies shown.

Discussion

Through my findings, it is seen that online harassment and cyberbullying is still a major trend. For both cases, females are highly more likely to be a victim as well as the crime to continue to happen offline, though more male victims are slowly emerging. Another interesting finding is females see online harassment to be a major problem, but strangely enough many choose not to respond to this crime. Social media also brings the ugly side of internet users. Whenever controversial topics are being discussed, people are automatically attacked if their opinion does not match the other individual. Strangely enough foul language and personalized comments are seen. With this happening, many choose to retaliate in the same manner, rather than relying on social media features. Very few will choose to report these comments to the platform or asked for it to be removed.

Cyberbullying in return is becoming more of a concern for parents and the schools they attended. Many parents feel their child has the potential of being a victim rather than being the perpetrator. It is interesting to note that many teens feel comfortable discussing cyberbullying with their parents. However, many felt that other authorities need to do more in addressing

online harassment or cyberbullying. Many feel social media sites, teachers, politicians, and law enforcers handle these crimes poorly.

This is important due considering online harassment and cyberbullying is still a rising trend. There are not many resources or concrete legislation that help prevent or mitigate these cybercrimes. Movements have been made such as bills being introduced in Congress after national incidents of children committing suicide or self-harming, but strangely no other actions have taken place. Also many existing laws regarding traditional harassment and bullying are vastly outdated. There is a lack of awareness and negligence within the federal level, which in return does not guide the criminal justice system. Law enforcers and judges do not know how to provide the appropriate amount of justice towards the victim. Meanwhile, schools are hesitant to interfere with students' behaviors shown online. Those events do not necessarily occur on school grounds, making it difficult to stop. There is also a strange element of students bullying strangers such as other minors or grown adults who have no connection with the students. Likewise how unknown students and adults will bully a student from a different school, despite having no reason to do so. This concept can also be applied to those facing online harassment. Employers and public establishments can only monitor so much on their employees' behavior. They can not necessarily stop their actions if it occurred during personal time or accounts. If solutions are not being created, the trend will still rise along with the number of victims. It may be better for social media platforms to provide resources towards victims experiencing these cybercrimes. This can help spread awareness as well as the rights they have on the platform, which is similar to how schools provide resources for victims of bullying. Likewise, clearer site policy can help lessen offenders' actions and their contact with their victims.

Limitations

The limitations of the studies are all data collected pertains to U.S. citizens only. Many cases dealing with online harassment and cyberbully are also underreported. Participants may feel comfortable speaking about their experience in surveys but did not necessarily report their situation to proper channels. By not doing so, agencies such as IC3 did not record their cases in their annual reports. Another limitation seen is there is not enough information about how exactly schools are handling the cyberbullying situation. Much data found just summarized general information such as stating teachers received training and resources found on school sites that parents and students can use. There is not much known if parents and students do use the resources but are not seeing improvement with their child's cyberbullying. Also, there are not many laws used to help prevent or de-escalate online harassment and cyberbullying. It is seen that many states do not update their laws to include these crimes. There has been a movement to introduce new laws about online harassment and cyberbullying, but it never moves on to the next stage. Rather they are added on as an amendment to the previous law, but do not accurately described these crimes, nor allow proper justice for the victims and their families.

Recommendations for Future Research

I would recommend future studies to analyze specific aspects of online harassment and cyberbullying. For instance, do online resources provided by either social media or school helped the victim, if so how. Likewise, were there incidents where these two entities did not help the victims despite them coming forth with their problems. Did they choose not to officially record their report or wrongfully punished the wrong individual in the scenario? I would also examine reasonings on why the government has not updated laws regarding online harassment and cyberbullying. Many laws have been introduced but were discarded for a multitude of reasons.

Conclusions

I have not necessarily proved my hypothesis to be true. It seems though offenders will target their victims regardless of what information is publicly known. However, social media do have a connection with cybercrimes. As seen in online harassment, there is slowly an increase in crime, especially towards male victims. Strangely enough, in cases such as these, victims choose to ignore the incident. With many people having different opinions, it seems that foul language and attacks on personal characteristics by strangers are becoming a norm. It is signifying that anonymity allows users to feel if they can behave in such a vicious way and the confusion on what is considered to be free speech. Controversial topics such as politics demonstrate how people will choose to behave negatively towards others since no immediate consequences occurs and more liklye not to face the victims offline. Mob mentality can also be used in these scenarios since like-minded individuals often choose to behave similarly to their peers.

Cyberbullying is still relevant more than ever. Any bullying occurring online will just continue offline and vice versa. With the popularity of social media, it unlocks more audiences to witness the bullying of minors online. Apps such as YouTube, Instagram, and TikTok attracts many young users. If their audience does not like the person or the content they are posting, vicious comments are made in hopes of the creator will see it. This opens a whole new avenue of offenders to attack these young creators. It is not only classmates participating in bullying the victim, but strangers as well. Unfortunately, adults will also behave similar to the victim's schoolmate, if not more. It is difficult to handle all the abuse from a large group of people when the victim lacks a support group such as close friends and parents. It is also difficult to try to stop strangers and adults from cyberbullying a minor considering many do not care about the child.

The debate of who is responsible for preventing or stopping social media crime is still ongoing. All parties including social media platforms do have some sort of responsibility for the crimes. For the victims, they should take advantage of their account settings and choose their privacy settings. Features such as unfriending, blocking, and reporting other users should be used if they are under attack or uncomfortable. It is best to avoid interacting with the offender if you can and set filters to avoid seeing comments or messages. Offenders, in theory, should not behave vilely online. However, it is unrealistic to believe perpetrators will not participate in these crimes due to social rules. Despite these individuals acting heinously, the consequences of their actions will occur, even if they do not understand the impact of their actions. If they continue to behave criminally, eventually they will receive their punishments in various forms, such as ruined reputations, loss of employment, and prison sentencing. Social media has the biggest responsibility. Their policies should be defined clearly as well as being strict enough for online harassment and cyberbullying to be not the norm. The platforms must have tools and features users can use to protect themselves while ensuring fair treatment is seen to all. They can help provide justice for the victims and deter perpetrators from committing the same acts.

References

2019 Internet Crime Report. (2019). In *Internet crime complaint center (IC3)* (pp. 1–28). Retrieved from https://www.ic3.gov/media/annualreports.aspx

A Publication of the National Center for Education Statistics. (2020). *Indicators of school crime and safety: 2019*. A Publication of the National Center for Education Statistics.

Anderson, M. (2018, September 27). A majority of teens have experienced some form of cyberbullying. Retrieved from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/

Bir, A., & Sodhi, S. (2020). *Social media law & cybercrime*. n.p.

Chahal, R., Kumar, L., Jindal, S., & Rawat, P. (2019). Cyber stalking: technological form of sexual harassment. *International Journal on Emerging Technologies*, *10*(4), 367–373.

Clement, J. (2018). U.S. social media user account privacy by age 2018 l Statistic. Retrieved October 11, 2020, from Statista website: https://www.statista.com/statistics/934896/users-have-private-social-media-account-age-group-usa/

Clement, J. (2019). Concerns about using Facebook in the U.S. 2018. Retrieved October 11, 2020, from Statista website: https://www.statista.com/statistics/1018760/facebook-user-concerns/

Clement, J. (2020a). Protection of devices and internet privacy 2019. Retrieved from Statista website: https://www.statista.com/statistics/463380/protection-of-devices-and-internet-privacy-worldwide/

Clement, J. (2020b). U.S. internet users who have experienced online harassment 2020.

Retrieved from Statista website: https://www.statista.com/statistics/333942/us-internet-online-harassment-severity/

Espelage, D. L., & Hong, J. S. (2016). Cyberbullying prevention and intervention efforts: current knowledge and future directions. *The Canadian Journal of Psychiatry*, *62*(6), 374–380. https://doi.org/10.1177/0706743716684793

Garett, R., Lord, L. R., & Young, S. D. (2016). Associations between social media and cyberbullying: a review of the literature. *MHealth*, *2*, 46–46. https://doi.org/10.21037/mhealth.2016.12.01

Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., … Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people. *JAMA Pediatrics*, *169*(8), 770. https://doi.org/10.1001/jamapediatrics.2015.0944

Hipp, J. R., Bates, C., Lichman, M., & Smyth, P. (2018). Using social media to measure temporal ambient population: does it help explain local crime rates? *Justice Quarterly*, *36*(4), 718–748. https://doi.org/10.1080/07418825.2018.1445276

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? an integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, *27*(4), 962–986. https://doi.org/10.1287/isre.2016.0671

Maeve Duggan. (2017, July 11). Online harassment 2017. Retrieved from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Michau, N. (2017). *Identity Theft Risk Quantification For Social Media Users*. University of Stellenbosch.

Pater, J. A., Kim, M. K., Mynatt, E. D., & Fiesler, C. (2016). Characterizations of online harassment. *Proceedings of the 19th International Conference on Supporting Group Work*. https://doi.org/10.1145/2957276.2957297

Pavlik, K. (2017). Cybercrime, hacking, and legislation. *Journal of Cybersecurity Research (JCR)*, *2*(1), 13–16. https://doi.org/10.19030/jcr.v2i1.9966

Perrin, A., & Anderson, M. (2019, April 10). Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018. Retrieved from Pew Research Center website: https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/

Prieto Curiel, R., Cresci, S., Muntean, C. I., & Bishop, S. R. (2020). Crime and its fear in social media. *Palgrave Communications*, *6*(1). https://doi.org/10.1057/s41599-020-0430-7

Salter, M. (2017). *Crime, justice and social media*. London and New York: Routledge.

Silva, L., Mondal, M., Correa, D., Benevenuto, F., & Qcri, I. (2016). *Analyzing the targets of hate in online social media* *. n.p.

Smith, L. R., Smith, K. D., & Blazka, M. (2017). Follow Me, What's the Harm? Considerations of Catfishing and Utilizing Fake Online Personas on Social Media. *Journal of Legal Aspects of Sport*, *27*(1), 32–45. https://doi.org/10.1123/jlas.2016-0020

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, *24*(1), 9–17. https://doi.org/10.2478/acss-2019-0002

Tariq, R., Irshad, S., & Soomro, T. (2018). Identity theft and social media identity theft and social media. *IJCSNS International Journal of Computer Science and Network Security*, *18*(1).

Wick, S., Nagoshi, C., Basham, R., Jordan, C., Kyoung, Y., Nguyen, A., & Lehmann, P. (2017). Wick et al -Patterns of Cyber Harassment and Perpetration among College Students in the United States a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License patterns of cyber harassment and perpetration among college students in the united states: a test of routine activities theory. *International Journal of Cyber Criminology*, *11*(1), 24–38. https://doi.org/10.5281/zenodo.495770

Wilcox, H., & Bhattacharya, M. (2020). A human dimension of hacking: social engineering through social media. *IOP Conference Series: Materials Science and Engineering*, *790*, 012040. https://doi.org/10.1088/1757-899x/790/1/012040

Wu, Y. (2018). Social media engagement in the digital age: Accountability or threats. *Newspaper Research Journal*, *39*(3), 287–296. https://doi.org/10.1177/0739532918796236