Online Peers Can Mean Offline Perils

Agatha Cristy L. Go
Makati City, Philippines
algo@apc.edu.ph

Kervi Ann S. Alfafara
Makati City, Philippines
ksalfafara@apc.edu.ph

Ma. Izza B. Javellana
Taguig City, Philippines
mbjavellana@apc.edu.ph

Ma. Elaine P. Lee
Las Piñas City, Philippines
mplee@apc.edu.ph

Nicson C. Nicolas
Laguna, Philippines
icnicolas@apc.edu.ph

***Abstract*—In the recent study, more than 80% of Web initiated crimes involve a social media platform (especially Facebook and Twitter). Moreover, 20% of active social media adults have complained about being a victim of cybercrime.[1] Criminals use social media to obtain important information like date of birth, location, background data, and more to target a victim. Burglary, identity theft and sex crimes are some of the major categories of Internet criminals. The Internet Crime Complaint Center (IC3), in partnership with the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), released a quantitative report on Cybercrime complaints during the year 2012 summing 289,874 accounts and $525,441,110.00 total loss from all over the world.[3] A variety of security organizations and government agencies respond to these complaints in the best possible ways, attaining justice at the end of the day. These groups also disseminate helpful information to the public of guidelines to avert harms, strongly believing in the "Prevention is better than Cure" principle. Organizations like the IC3 and the FBI will continue to take action and certainly create solutions to impending cybercrimes.[2] The paper seeks to visualize the future of social networking sites, as well as determine future attacks and its corresponding remedies.**

Keywords: **Social networking sites, Security, Cybercrime**

I. INTRODUCTION

Social networking websites, also referred to as social networking sites (SNS), are online platforms that allow users to create a public profile and interact with other users on the website.[5]

SNS is built upon the concept of the real world social network through the use of mutual activities and interests and functions as an online community for Internet users. SNS can be a useful platform for communication and is a sea of information. It can also serve as an entertainment, as some SNS can connect a user to games and applications that might suit his interests. Some of the features vary depending on the SNS which include photo/post sharing and comments, messaging and online/video chats, free games and applications. Nowadays, connecting to the Internet world can be as easy as just a click away. Personal computers, laptops, even mobiles, with Internet connections, can connect a person easily to these SNS. In the recent research, 73% of the adults ranging from 18-65 y/o use SNS. Some of the most popular SNS are (1) Facebook which top the list with 71% adult users, (2) Twitter with 18%, (3) Instagram with 17%, (4) with 21%, and (5) LinkedIn with 22%.[6] Nonetheless as advantageous and helpful SNS can be to its users, it can also bring danger without the right knowledge about what to know and what are the things to share and not to share on these sites. Publicity of information can lead to serious cases like identity theft, identity fraud, scams, and more.

II. PROBLEM STATEMENT

With an increasing amount of social networking sites users every day—of various types and intentions, comes a growing rate of cybercrimes transpiring. Many victims have reported several kinds of crimes that took place in popular social networking sites; sending queries, claiming to be friends, etc. are common procedures for initializing an unlawful act.[2] Most of the complainants are unaware that they have been exploited until discovery.

By definition, scam is a quick-profit scheme where a person cheats another individual or group out of money by presenting them with false information during a deal or offer.[17] A user or person can be scammed in many different ways. Focusing on the SNS, scams can be those links with enticing title or thumbnail of a video or photo that may be of user's interest and when clicked, it may ask the user to allow to use his personal information or enter a bank account number to know where to send the money that the user may claim if he wins the game as what the scammer might reason out. It may also be a special mention or direct message of a link from anonymous users in Twitter or a friend request from a random person in Facebook. The highest percentage

of scams victims are adults aged 30-39, least with those aged 60 and above. It may be obvious to determine whether a site or account is a scam but the number of victims increases yearly compared to the previous years' statistics.[27] This only means that some of the people can be very much unaware of what they're getting themselves into online.

Bullying isn't prevalent only in the real world, currently the advancement of the technology and the Internet are being used as a form to bully other people. Cyber bullying is bullying behavior (tormenting, threatening, harassment, etc.) that takes place through electronic mediums, including the Internet and mobile phones.[7] This form of bullying can take on various forms including (1) sending harsh, rude emails and comments, (2) spreading false rumors on the SNS, (3) using fake profiles to impersonate and harass others and (4) spreading sexually and unflattering photos of one person.

Cyberbullying can affect all races and genders of any ages, however most of the times it is the teens who suffered most. Teens become aggressive and violent that leads to serious and even deadly repercussions for others. According to the recent study of i-Safe Foundation, 7.5 million users of Facebook are under age 13. 1 out of 10 teens have experienced cyberbullying threats on this website, adding up to 800,000 kids. 25% said that they are repeatedly bully on the Internet. While according to Pew Internet, 55% of teenagers witness bullying on social media, while 95 percent of teenagers who have witnessed this bullying have seen other ignoring this behavior.[8]

While teens frequently and normally use SNS to stalk other people, cyberstalking is beyond just following their activities in Facebook and any other SNS. Cyberstalking refers to harassment or unwanted communication via some form of technology including computers, global positioning systems (GPS), cell phones, cameras and more.[9] Cyberstalkers use SNS news feed, profile page, chat rooms and more to trail the current actions of the victim.

In recent studies, women are more likely to be stalked than men. 80% of stalking cases happened to women, while there were only 20% cases for men. 75-80% of stalkers are men stalking women. 36% age 18-30 years old are victims of cyberstalking and 69% of the victims are single. The cases escalated quickly as Facebook is primarily being used to stalk with 22%. Following others activities through personal website of the victim garnered 11% and Twitter 3%. [10]

Online robbery is just the same as the actual robbery. The only difference are the means of doing it. It is a crime of taking or attempting to take something of value by force or threat of force or by putting the victim in fear. At common law, robbery is defined as taking the property of another, with the intent to permanently deprive the person of that property, by means of force or fear.[18]

It doesn't take much for a thief to find out where you live, go to school, work, or hang out if you make that information readily available on SNS. For instance, if you use Facebook's check-in or Google Maps feature, then you could be in a heap of trouble if a robber is paying attention. This person isn't always a complete stranger either; they may be an old acquaintance or someone else you'd never expect to come rob you. 78% of burglars use Facebook, Twitter, and Foursquare to target potential properties, while 74% of burglars use Google Street View to scope out potential homes before they strike.[19]

However, most of the time, robbers use SNS and other online means to rob banks. According to one of the reliable news website, a bank was robbed by hackers who gained access to it site's database by disguising their identities through social engineering attack. Thus, the hackers was able to rob $1.3 Million.[20] Undoubtedly, online robbery is one of the most common crimes done online.

People can be very careless about their personal information that they'd very much rely with the social networking platforms and believing that no one would take interest on the publicity of some of their personal information such as their real names, age, birthdate, address, etc. Identity theft is when your personal details are stolen and identity fraud is when those details are used to commit fraud. Identity theft was the #1 complaint category in the Federal Trade Commission's (FTC).[22][23]

According to a recent research, identity theft affects millions of people a year, costing victims countless hours and money in identity recovery and repair.[24] SNS are mostly the medium of these identity thieves as information of a particular person can be in public and can be freely exploited without having the user notice it. Since most people don't have enough knowledge on security education, they're more likely exposed on these cases. According to FTC source, the highest percentage of identity theft victims were age 20-29 while children, aged 19 and under, made up 6% of all identity theft victims in 2012. 54% of the victims are targets of identity threat, 13% are "socially engineered" to disclose password or other sensitive information, 15% had their accounts accessed without their permission, and 70% were asked to visit a scam website via a private message.[22][25]

Defamation is a false and unprivileged statement of fact that is harmful to someone's reputation, and published "with fault," meaning as a result of negligence or malice. There are 2 specific ways of defamation by law, 1.) Libel is a written defamation and 2.) Slander, spoken defamation.[26] Defamation is the 6th out of the top 7 most common crimes happening on Facebook.[19] In relevance to SNS, users can easily post false stories or accusations about another person may it be intentional or not. The victim can file a lawsuit against the user who posted it as defamation is a case recognized by law. An individual commits the crime of defamation when they communicate a false statement to a third party that paints another individual or entity in a negative light.[19]

There is an immense need to respond to these issues as they are expanding and becoming more and more complicated that the state may be unable to resolve them as time progresses. Despite actions sent by the government and credible organizations, a vast percentage of unsolved cases is still alarming. Hence it is high time to formulate more effective solutions for present crimes, as well as combat for succeeding methods.

III. RESULTS AND DISCUSSION

Indeed, SNS has completely revolutionized the way people interact. However, there's a dark side to the world's love affair with social media. Criminals are finding new ways to utilize SNS to commit new and disturbing crimes that authorities don't necessarily know how to police. Thus, the key to fully enjoy social media is the awareness about the common crimes committed on SNS so everyone can avoid being a victim.

This study aims to provide safety measures on how to solve as well as prevent the existence of the most common crimes done using SNS and these are: Scams, Cyberbullying, Cyberstalking, Robbery, Identity Theft, and Defamation.

Never click on suspicious links on social networking sites – even if they are from close companions, as they may be scams and your peers may have been victimized. Doing so will prevent the user from participating in the activity. If, however the link is from a trusted friend or has an identifiable URL, accessing it may mean no harm to you.

In Cyberbullying, (1) Never share information online if it could be used against you. Cyber bullies often use pictures, status updates, and personal information they find online to harass their targets. It's fine to share a little information about oneself online, but never reveal something the world doesn't have to know. (2) Be mindful of one's tone when communicating online. Sometimes online communications can be misread by the recipient, leading to a conflict that can escalate into a bullying situation. Be respectful to people one communicates to online to avoid making enemies. If a conflict develops, try to resolve it in person. (3) Don't participate in cyber bullying behavior. Even if all of one's friends are doing it, cyber bullying is still wrong. People choosing to go along with the crowd in cases of cyber bullying is what makes these types of attacks so effective and damaging. One's behavior can influence other people's actions; make it clear that to not stand for cyber bullying by setting a good example for others. (4) Don't wait too long to ask for help. One might be tempted to let the bullying run its course instead of bringing attention to the problem, but in doing so the bully will get the message that there's no penalty for putting someone else in danger. Don't assume the problem will go away on its own; speak up immediately to put a stop to it.

To combat Cyberstalking: (1) Only "friend" real friends. Don't accept a friend or follow request from a stranger - people are not always who they say they are and the best way to keep scammers out is to never let them in. Likewise don't answer social media messages or even cellphone texts from people or numbers you don't recognize. (2) Set online social networking profiles to private. Never share account details with others and regularly update the computer's security software. In choosing to not set some accounts to private, one must remember to be extra cautious about what to share and who to connect with. Think about who will be seeing the information one posts. If privacy settings are not controlled, one will be giving information about oneself out to anyone with access to the Internet. (3) If a user is receiving unwanted contact, make clear to that person to not contact again. Many women who have reported being harassed do this and warn that any further contact will result in the filing of a police report. Depending on the harasser, engagement with the person can escalate or cease, so if one considers contact appropriate and necessary, do so once and document it. (4) Tell family and friends that about online prowler. Being stalked – online or offline – is a traumatic experience and support from family and friends is critical at this time to help cope. Also check what the pursuers are revealing about the user and one's possible relationship in the stalkers' online spaces, albeit inadvertently. (5) Check out investigators in Cyberstalking cases. Identify which bodies or agencies are available in the country and community that can take action in such cases. Contact the police or other relevant agency and inform them of the situation in as much detail as possible, providing copies of documentation of the harassment.

In order to prevent such unfortunate event as robbery through the Internet, be cautious and discreet. Do not easily be deceived by any means of money request sent to a user even if it appears from any of the family members or friend. Before giving personal details, especially account information, scrutinize first the event. If the sudden money request appeals skeptical, do not hand over any information.

Countering Identity Thieving: (1) Don't use lazy passwords. Hackers will easily detect common passwords. To prevent such event, form a strong password by using alphanumeric, symbols, uppercase and lowercase combination. By this means, brute force attack will take a long time before hackers can decipher the password. (2) Do not use the same password for different accounts. It's almost tough to remember passwords from different accounts, hence users tend to use the same password for all of the accounts they have. To counter this, come up with a base password and tack a logical modifier into it, for an instance on Facebook, use fbThisIsMyPass2014, on twitter, twitThisIsMyPass2014. (3) Fill out only the necessary fields. When signing up on a SNS or any website, installing a software read the fine print. Some sites require you to give personal information. Only fill out the fields marked with asterisk (*) in it and leave others blank. (4) Do not give full personal information about

oneself. To avoid any untoward instances most especially identity theft, give only a little about the user. This applies most in chatrooms, SNS or when negotiating, or deals through meet up sites. (5) Try not to access social networking sites on public computers. Use own computers or smartphones instead of the computers at libraries and other public places. Login information can be intercepted. (6) Grant access cautiously. Apps often asked you to sign in to some SNS account, in doing so you are granting these third party apps to gain access control of your account. Before allowing it, research first the apps on Google and find out if others encounter unnecessary instances with it.

Defamation prohibition: (1) Be aware of what to convey. In defamation cases, one is liable not just for what one says expressly, but what ordinary people will read between the lines. One is also liable for publishing a defamatory statement made by someone else, albeit accurate quotations. A user needs to identify any "stings" in what to write the barbs that affect someone's reputation. What will ordinary, reasonable, fair-minded people take it to mean? (2) Control the meaning. The first battle in a defamation case is usually over what the words mean. Don't leave this to chance. Plaintiffs like to exploit ambiguity, claiming that the audience will understand it in a defamatory sense. One should try to eliminate ambiguity and convey your meaning precisely. (3)Only say what one can prove. Truth is usually the most important defense in a defamation claim. Ask oneself what evidence one could put before a court if someone ignites a challenge, and how convincing that evidence would be. (4) Use the language of opinion. There's a defense called honest opinion (it used to be fair comment) for those who are expressing genuine opinions on accurate facts that are set out or understood by the audience. So make it clear that one is expressing or republishing a view. Say "I think", "he believes", "she reckons", "they claim". Say whose opinion it is. Use phrases that are evaluative, not factual – "I think his behavior was disgraceful". Use rhetorical questions rather than assertions of fact. Use visuals to clue readers in to the fact that they're getting opinions, as in a letters to the editor page. Instead of making factual allegations, use the word "seems" or "appears", which at least opens the door for an opinion defense. (5) Bear in mind who to deal with. Some people are much more likely to sue than others. Politicians, for example. Business people. Celebrities. People whose reputation is important to their livelihood and have the resources to take action. Also, take extra care writing about police, journalists, and even lawyers.

The Federal Bureau of Investigation, Internet Crime Complaint Center, and National White Collar Crime Center are the organizations responding to complaints from users who are victims of cybercrimes. The said groups provide training, investigative support, and research to combat emerging economic and cybercrime problems. The NWC3 informs the general public of methods that prevent online crimes from happening to them. The IC3's purpose is to serve as a central hub to receive, develop, and refer criminal complaints regarding the rapidly expanding occurrences of cybercrime. The latter organization gives the victims a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations on the internet. [3]

IV. CONCLUSION AND RECOMMENDATION

Social Networking Sites or SNS is defined as an online platform that allows users to create public profile and interact with other users on the website. It is merely used for communication and sharing of interests. This paper focuses on how these SNS are being used by people to exploit users' information and use it maliciously. Without enough knowledge on the importance of security, it might lead to serious cases such as Identity Theft and Fraud, Scams, Cyber bullying and Harassment, Cyberstalking, Defamation, and Robbery. Discussed in the problem statement, these cases related to SNS have something in common when it comes to its causes. It is the publicity of important personal information of a user and how victims initially allow intruders to be able to see their information. Accepting friend requests from people you don't know or specifying information such as where you are at a particular time can be used by someone who has unwanted intentions.

Identity Theft, Fraud, Scams, and Robbery cases need the personal information of a user and are usually attained by a click of a link that would eventually ask the user to enter some important information, responding to 'financial' inquiries of a person who messaged a user, posting information about current whereabouts, companions, and activities. While cases such as Cyber Bullying and Harassment, Cyberstalking, and Defamation includes the responsibility of users of the things they post and share with their friends on SNS that may be offensive to others.

This case study therefore concludes that right privacy of important personal information of every user and the need of security knowledge of everyone should be encouraged. Every netizen should know what things to share or whatnot, and know how things can go wrong with SNS more than they realize. There are current laws applicable to online activities, therefore users must know how to act within the limits of it.

As part of the authors' research, the following are some recommendations to combat cybercrimes: (1) Parental Control software such as Norton Family, Bitdefender, Net Nanny, etc. are very useful in keeping young netizens safe while browsing the internet. (2) Fraud Prevention tools are also available and are being used mostly by banking industries. (3) Prevention tools for network harassments and spams are also available. Its method is to block email domains and IP addresses. (4) Lastly, education and training are the simplest manners to avert cybercrimes.

V. REFERENCES

[1] I. Ahmad. (2013, October 2). Are You Safe on Social Media [Online]. Available: http://socialmediatoday.com/irfanahmad/1786586/social-media-crime-are-you-safe-social-mediainfographic

[2] The FBI. Social Networking Sites: Online Friendships Can Mean Offline Peril [Online]. Available: http://www.fbi.gov/aboutus/investigate/vc_majorthefts/innocent/social-networking-sites

[3] IC3. 2012 Internet Crime Report [Online]. Available: http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

[4] B. Dinerman. (2011). Social networking and security risks [Online]. Available: http://www.gfi.com/whitepapers/Social_Networking_and_Securit y_Risks.pdf

[5] Definition of: social networking site [Online]. Available: http://www.pcmag.com/encyclopedia/term/55316/socialnetworking-site

[6] J. Brenner. (2013, December 31). Pew Internet: Social Networking (full detail) [Online]. Available: http://pewInternet.org/Commentary/2012/March/Pew-InternetSocial-Networking-full-detail.aspx

[7] stopbulying.gov (US). Cyberbullying [Online]. Available: http://www.stopbullying.gov/cyberbullying/

[8] NoBullying.com (UK). Cyber Bullying Statistics [Online]. Available: http://nobullying.com/cyber-bullying-statistics/

[9] Safety Web (US). [Online]. Available: https://www.safetyweb.com/cyberstalking

[10] WHOA (US). 2012 Cyberstalking Statistics [Online]. Available: http://www.haltabuse.org/resources/stats/2012Statistics.pdf

[11] R. Jenkins and Co. How to be safe on the Internet [Online]. Available: http://www.wikihow.com/Be-Safe-on-the-Internet

[12] TheJudge121 and Co. How to Stop Cyber Bullying [Online]. Available: http://www.wikihow.com/Stop-Cyber-Bullying

[13] M. Johansson (2013, November 4). Social Media Scams: 11 Tips to Fight Them [Online]. Available: http://socialmediatoday.com/mike-johansson/1886166/social-media-scams-how-to-fight-them-11-tips

[14] A. Lagura and Co. How to avoid Social Networking Scams [Online]. Available: http://www.wikihow.com/Avoid-Social-Networking-Scams

[15] M. Hoal (2012, March 22). 5 ways to Handle and Prevent Cyber – Harassment [Online]. Available: http://abcnews.go.com/Technology/We_Find_Them/ways-handle-prevent-cyber-harassment/story?id=15973742

[16] S. Price (2013, November 26). How to avoid Defamation [Online]. Available: http://inforrm.wordpress.com/2013/11/26/how-to-avoid-defamation-steven-price/

[17] Free Internet Security. What is Scam? [Online]. Available: http://www.securitysupervisor.com/security-q-a/online-security/263-what-is-scam

[18] Wikipedia. Robbery [Online]. Available: http://en.wikipedia.org/wiki/Robbery

[19] The Best Degrees. 7 Common Facebook Crimes [Online]. Available: http://www.thebestdegrees.org/7-most-common-facebook-crimes/

[20] L. Bicchierai (2013, November 9). $1.3 Million in Bitcoin Stolen in Major Online Robbery [Online]. Available: http://mashable.com/2013/11/08/bitcoin-theft-tradefortress/

[21] Free Internet Security. What is Scam? [Online]. Available: http://www.securitysupervisor.com/.../263-what-is-scam

[22] N. Mannino (2013, November 13). Identity Theft Statistics: Why You Should Be Alarmed [Online]. Available: http://www.creditdonkey.com/identity-theft-statistics.html

[23] Action Fraud (UK). Identity fraud and identity theft [Online]. Available: http://www.actionfraud.police.uk/fraud.../identity_fraud

[24] Entrepreneurs Organization (USA). How Social Media Networks Facilitate Identity Theft and Fraud [Online]. Available: http://www.eonetwork.org/.../social-media-networks...

[25] ITRC. ITRC Fact Sheet 138 Social Networking and Identity Theft [Online]. Available: http://www.idtheftcenter.org/Fact-Sheets/fs-138.html

[26] Electronic Frontier Foundation(USA). Online Defamation Law [Online]. Available: https://www.eff.org/.../bloggers/legal/liability/defamation

[27] Consumer Fraud Reporting (USA). Internet Fraud, Scam and Crime Statistics – 2009 [Online]. Available: http://www.consumerfraudreporting.org/internet_scam...