About Author

The Book ‘’ Cybercrime and Social Media Relationships’’ is written by Cyber security expert Mr. Joseph Thachil George. Joseph writes books, which, considering where you’re reading this, makes perfect sense. He is best known for writing research papers, including the technical and non- technical contents.

Joseph has taken bachelor’s degree in Computer Science and Engineering from the Mahatma Gandhi University in Kerala, India, and he holds M.S in Cyber Security from the University of Florence, Italy. At present Joseph is doing research in Cyber security and blockchain.

Joseph has seven years of experience in computer science and engineering field and he also done research projects for various Italian companies and governments such as IGT-Rome, Comune di Palermo, Italy, Confesercenti Rome.

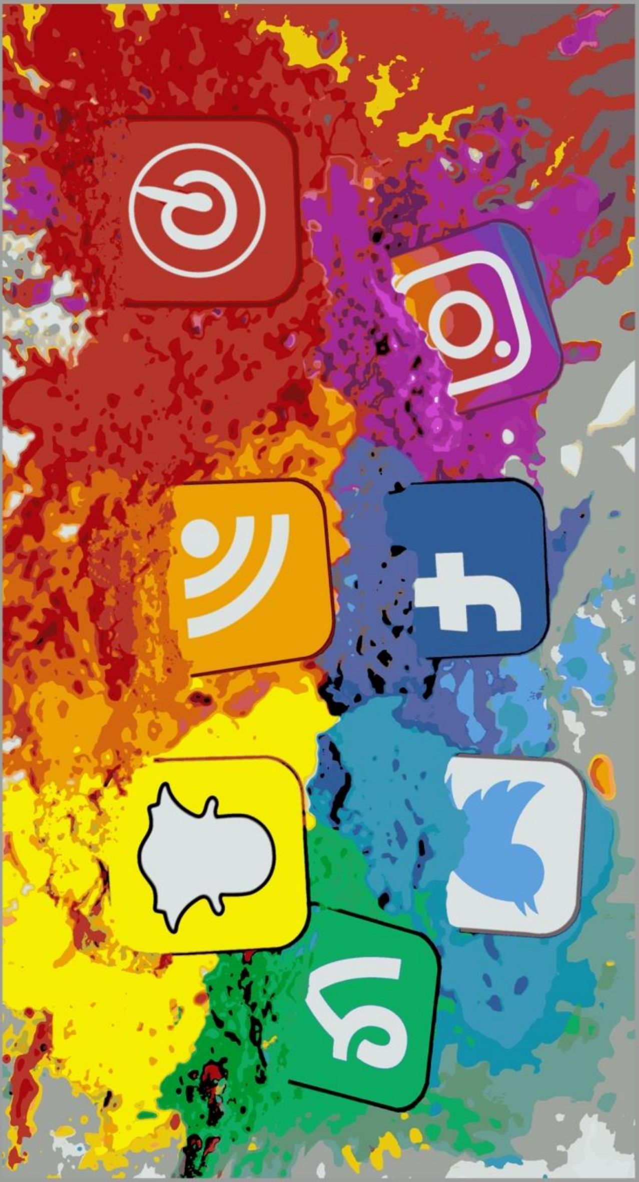
Table of Contents

PAGES

CHAPTERS

Students

- Think before making every post online, and avoid making posts that can have a negative effect on your reputation.
- Learn what cyberbullying is and what behaviors are involved in cyberbullying.
- Avoid putting inappropriate photos online because they can be the fuel that cyberbullies use.
- Messages from unknown people without opening them. Also, avoid opening messages from known bullies.
- Treat everything and everyone with respect.



Social Media Safety Tips

While the internet can be a great resource to help students prepare for tests and do research for assignments, as well as stay in touch with their friends, it's still important for them to be safe when using technology — especially social media sites. The following are some tips to help teens stay safe when using social media.

- Never give other people password information.
- Don't post address, telephone number or school location online.
- Use strong privacy settings, so only friends and family can see posts.
- Be careful when clicking on links, and don't click links from unknown people.
- Don't accept friend requests from strangers.
- Use strong passwords and change them regularly.
- Don't respond to abusive posts.
- Never open attachments from unknown people.
- Set up security questions on social media sites.
- Don't allow programs to track location.

7 Connection between SOCIAL MEDIA & SEX

Introduction & Study Methods

With the increase in technology use, it is important to understand the landscape of trafficking online. The Research Subcommittee of the Ohio Attorney General's Human Trafficking Commission was asked to conduct a study to gain a better understanding of how social media is used to connect, recruit, and sexually traffick youth. Therefore, researchers at University of Toledo in the Human Trafficking and Social Justice Institute designed and obtained university approval for this qualitative study.

Researchers interviewed knowledgeable professionals from the Ohio Anti Human Trafficking Coalition Network, then used snowball sampling, asking participants if they knew any other knowledgeable professionals who might be willing to participate. In total, there were 16 in-depth interviews conducted with participants that included knowledgeable members of law enforcement, judges, direct service providers, advocates, and researchers that had engaged victims that were trafficked online.

Screening questions were used initially with participants to determine eligibility, and knowledge about social media as a means to connect, recruit, and traffick youth. For those who were eligible, interviews were conducted over the phone and audio recorded using Google Voice or a traditional handheld recorder. Interviews lasted between 25 minutes to an hour. All participants were asked the same series of questions and asked to clarify or expand on some responses when necessary.

Completed interviews were transcribed verbatim, and transcriptions were analyzed line-by-line. From this analysis, codes were identified, and codes were collapsed into themes.

Findings

The Process

There are innumerable websites and applications designed to build community and connect users to new people. Any site that allows users to connect to people with numerous motives and intentions is an inherently risky site. However, most experts agree, the vulnerability of the user elevates risk. One professional reports, "It feels less about the app and more about the person's vulnerabilities. I think when I get a friend request from a person I don't know, it doesn't even occur to me to start a relationship with someone that way, but I have a different background than many of these women. I think the risk is high because they are often looking for someone who can nurture them, care for them, and then so they are extremely vulnerable" – Ohio Anti-Trafficking Professional, 2018.

The Internet and social media allows traffickers to quickly connect with vulnerable youth. One professional explains, "These guys are just master manipulators at making these, figuring out these girls vulnerabilities and insecurities and making them feel unloved...They use the app to watch for people that are sending out signals of what is going on in their life, and kids put a lot of stuff out there. There is a point where this girl goes from being out of sorts about her life at home...to fast forward six weeks and...she's in Fort Wayne, Indiana doing commercial sex

Self-Erasing Technology and/or Developing a Second Persona

Self-erasing technology or second persona profiles allow for communication with traffickers to be hidden and avoid suspicion from others.

"Kids will create what they call finstagram accounts that are fake Instagram accounts that their parents aren't aware of. So they have a completely squeaky clean Instagram account and then another alternative account, and a lot of exploitation can happen there." – Ohio Anti-Trafficking Professional, 2018

"...the mass IP self-erasing tech system..., they can organize and meet, and even if the phone is confiscated it can be very difficult to recover that information and make your case." – Ohio Anti-Trafficking Professional, 2018

"...the individual was able to migrate the conversation over to one of those [less familiar social media sites] by saying, 'you don't want your parents to find out what we're talking about,' and so they will use that fear of repercussions as a way to compel the youth, coerce the youth, and utilize those tools [applications]." – Ohio Anti-Trafficking Professional, 2018

15

Criminal Use of Social Media

Defining social media is difficult because it is ever changing like technology itself, but for the purposes of this paper, social media will be defined as any website or software that allows you to receive and disseminate information interactively.

The tremendous rise in popularity of social media over the past seven years has led to a drastic change in personal communication, both online and off. Comparing to the world population clock, the total world population is around 7.06 billion.1 With that being said, the popularity of sites such as Facebook, (1.06 billion monthly active users)2, YouTube (800 million users)3, Twitter (500 million users)4, Craigslist (60 million U.S. users each month)5, and Foursquare (has a community of over 30 million people worldwide)6 has connected people from all over the world to each other, making it easier to keep in touch with friends, loved ones, or find that special someone. In addition to personal usage, businesses and the public sector use social media to advertise, recruit new employees, offer better customer service, and maintain partner ships.7 In fact, 65% of adults now use social media.8 Social networking is the most popular online activity, accounting for 20% of time spent on PCs and 30% of mobile time.9 As social interactions move more and more online, so does the crime that follows it.

Crimes Linked to Social Media

Social networking consists of websites that allow users to create an online profile in which they post up to the minute personal and professional information about their life that can include pictures, videos, status updates, and related content. Social networking is a potential gold mine for criminals who leverage the users' personal details into financial opportunity.

Crimes Linked to Social Media

Social networking consists of websites that allow users to create an online profile in which they post up to the minute personal and professional information about their life that can include pictures, videos, status updates, and related content. Social networking is a potential gold mine for criminals who leverage the users' personal details into financial opportunity.

Burglary via Social Networking

The classic example of exploitation on social networking sites involves the perpetrator perusing users' profiles and looking for potential victims in the vicinity who won't be home. Myspace and Facebook users can post that they will be out for the evening, which gives potential thieves a large time window to burgle the property. Facebook and Twitter now have a new "my location" feature allowing readers to see where they were and how long ago it was when they posted their update, making it that much easier for criminals to attack.10 Stories of this nature are frequently in the media11 and serve as a reminder that users are not as cautious as they should be with their personal information. The thieves see a status update of a family being on vacation for an extended period of time and jump at the perfect opportunity to steal some valuables.12 Another example of a recent investigation in New Hampshire ended when thieves who used Facebook to profile victims, were caught using a very peculiar type of firework that was recently taken in a burglary. An off-duty officer investigated firework explosions he could hear in the distance. The fireworks were stolen in the series of break-ins over the prior month.

Some other social networking applications, such as Foursquare and Gowalla are primarily location-based networks. Users of these networks can be rewarded for posting their locations frequently and are then given temporary titles while at their location--for example, posting that you're having a cup of coffee at Starbucks may make you the Mayor of Starbucks on this certain site.14 As previously mentioned, posting a location allows perpetrators the perfect window to commit a burglary, vandalism, or even a home invasion.

Phishing & Social Engineering

A variety of forms of identity theft are performed daily on social networking sites under the guise of other tasks. For example, one technique is called phishing, which involves making attempts to acquire passwords, account numbers, and related information. It is said that phishing has become the most widespread Internet and email scam today.15 The term is a play on the actual sport of "fishing," in which perpetrators send out many (sometimes millions) of emails with the hopes of getting "bites" in return. Despite the low success rate, criminals continue to send out emails that look like legitimate concerns over account security or sale reminders from your favorite retailer.16 Beware of the requests to discontinue emails that you believe are scam, this is a way that phishers can tell if an email is still active or not. Phishers can take this request to discontinue, note that the address is a true email address, and send more scams from a new account. In 2012, there were nearly 33,000 phishing attacks globally each month which totaled a loss of $687 million. These phishing attacks mark a 19% increase globally compared to the first half of 2011.

Another technique of crime on social networking sites is social engineering. In a classical sense, social engineering refers to the social manipulation of large groups of people to meet political or economic ends. Today, it has taken on an additional meaning in the cyber security world. Social engineering refers to gaining access to information by exploiting human psychology rather than using traditional hacking techniques.18 A classic example of this starts with a friend on your network sending you a message asking for a quick loan to get car repairs so he/she can get home for work on Monday, and ends with you finding out a few days later that your friend never needed car repairs and that the person you transferred money to was a scam artist. This form of social engineering is surprisingly easy to achieve, and because of it, the computer security firm Trend Micro calls Facebook a "minefield of scams."19 All that is needed by the scammer is the username and password of one member of a network and a little practice in writing letters that sound urgent to inspire friends to aid you. All the while the scammer is vague enough not to reveal the impersonation. Even if only a few friends on the list are duped, the return on investment for the scammer is quite high. Social engineering isn't limited to social networking. A recent case involved the software company Oracle. During a convention, a contest was held to demonstrate the dangers of social engineering. Several hackers posed as IT professionals and asked company employees to hand over data and visit websites as part of "routine IT protocol." Oracle employees as well as many others were frighteningly compliant in the demonstration.

Malware

Last, social networking offers opportunities for virus and malware users. Users clicking on links, opening attachments, and responding to messages on networks can become victims without knowing it, resulting in adware, viruses, and malware being loaded onto their machines. Malware attacks have increased and are only growing because of the use of social media. According to one report, 52% of organizations have experienced an increase in malware attacks as a result of their employees' use of social media.21 Additionally, the business world is concerned that their employees' online behavior could be putting their

network security at risk. Sophos' 2010 Security Report surveyed over 500 organizations and found that 72% were concerned that social networking endangered their security.22 A 2011 survey done by Socialware found that 84% of financial advisors said they use social networks for business purposes, up from 60% in 2010.

While there is very little risk of contracting malware from Facebook itself (or any other reputable social media site), there are various tricks that scammers can use to get you to leave the protective social media environment without even realizing it. A user must first be tricked into leaving the Facebook world by clicking a link on Facebook that leads to an external website, then a malware attack is able to take place.24 One technique criminals use to trick users into installing malware is by creating fake pop-ups that look like update screens used by various common web browser plug-ins (such as Adobe Flashplayer), in hopes that users will be used to occasionally updating their software for websites and click on it without a thought.25 The Sophos' Security Threat Report of 2013 states that in 2012, more than 80% of threats were from redirects, mostly from legitimate sites that had been hacked.

Cybercasing the Joint

Another development in social media technologies is called geotagging, which embeds geographical data (longitude and latitude) into media such as photos, videos, and text messages.27 Geotagging allows users' locations to be posted along with their media. The location of users can be found quickly and precisely by combining the geotagging of media-friendly sites, such as YouTube, Flickr, Google Maps, Twitter, Facebook, and Craigslist, with all the aforementioned networking sites to triangulate all positions known.28 Facebook snuck in the "add location" option without letting users know. This feature tacks on information about where the user was and when they were there when they updated their status. For example, at the end of a status it will say "near Cheat Lake approximately 2 minutes ago."29 This same feature has been added to Twitter, only before composing a tweet it asks whether or not you would like to add your location,30 a tad more considerate than Facebook, but dangerous nevertheless.

A recent study from the International Computer Science Institute tested the potential to use all publicly available resources to determine the locations of a variety of people on the Internet.31 A process called cybercasing allows users to access online tools to check out details, make inferences from related data, and speculate about real world locations for questionable purposes. Cybercasers use the Internet to determine the location of a desired victim by accessing.

1. The first scenario used the virtual flea market site Craigslist to spot desirable photographs with geotagged data. In most cases, the researchers were able to cross-reference Google Street View to determine the exact address of the poster. Researchers also determined what times were best to burgle a residence by a poster's ad that would often state "Please call after 5 p.m.," implying that they would be gone at work on most days.

2. The second scenario examined the Twitter feed of a well-known reality show host. By viewing the pictures posted on TwitPic with the Firefox plug-in Exif-Viewer, the researchers only had to right click on the celebrity's pictures to reveal geographical coordinates. By taking the average of several pictures posted in a similar region, the researchers could determine the location of the user with great precision.

3. Lastly, YouTube was used to find the home address of someone currently on vacation. By creating a script that collects usernames and downloads the related videos, researchers were able to find a user that lived in the predetermined area of Berkley, CA, and was currently on vacation in the Caribbean, as determined by his most recent YouTube uploads. The researchers were able to use his real name in a Google search to determine his address. The entire process took less than 15 minutes.

Costs and Statistics

The prevalence of criminal activity on social media sites is difficult to determine. In fact, there are currently no comprehensive statistics on social media crimes, although

Conclusion

Social networking can be a great experience for all of us but also has clear risks. They may forget who they are communicating with and who might see their posts.

They also may feel braver to say and do things online that they might not do offline—including talking to and confiding in strangers. It is important that your child understands the risks associated with disclosing information about themselves and how to manage their privacy and online 'friends'.

In turn, it is important that you are aware of how you are interacting with others on these sites and equip them with the skills to manage negative situations, which include:

- cyberbullying
- not protecting their own privacy
- sharing information with people they don’t know or trust
- losing control over where a photo or video has been shared
- identity theft
- seeing offensive images and messages
- meeting people in real life who they only know online
- unwanted contact by strangers or predators.

This book will really help you to choose wise decisions while using social media.