DETECTION AND PREVENTION OF SOCIAL MEDIA CYBERCRIME AMONG STUDENTS

A. Lawal, N. Cavus
Near East University, Department of Computer Information Systems (CYPRUS)

Abstract
The wide acceptance of social networking sites motivates students to use it for entertainment, finding and chatting with friends, sharing photos and videos, post happenings and events in real-time. Presently, millions of students connect to social networking site every day. This makes the criminal elements in the society trick the students by using their information available on the social networking sites to commit crime against them. This research investigated the types of crimes that are committed to students on social networking sites. Also, the researchers investigated the ways and techniques used by these criminals to commit crime against the students. At the same time, the research also investigated the various ways and techniques the students can use to detect, prevent and also to mitigate the impact of such crimes against them. Literature review showed that mostly kidnapping, sexual harassment, bullying, credit card fraud and threatening crimes that are committed to students on social networking sites can be avoided. The various ways and techniques used by the criminal to commit crimes against the students such as identity theft, phishing, spam etc. were also identified. Similarly, the various techniques like parental controls used in Facebook, TheOneSpy monitoring app used in Whatsapp that are used to protect the students were discussed. At the same time, computer forensic data analysis techniques used to detect crime against the students was analyzed. The researchers hope that this paper would be a guideline to students, parents and teachers in protecting the students against the menace of social networking sites.

Keywords: Social networking sites, cybercrime, crime detection, crime prevention, computer forensic.

1 INTRODUCTION
Social networking sites is a platform which people used in promoting ideas, disseminating information, maintain interpersonal relationships, tract organizational items, manage staff information, create people awareness, respond to distress peoples call by the security agencies ([1], [2], [6], [8]). Social networking sites has grown exponentially in the last decades to change the way billions of students conduct their activities and interact with each other, share personal information, create online personal profiles which resulted in the accumulation of large volume of data which also paved the way for opportunities in research and educational activities ([5], [27]). The wide acceptance of social networking sites allows billions of users including students, educators as well as people with questionable characters to share photos, videos, post happenings and events, find and chart with friends, create, and disseminate ideologies and knowledge [27] in real-time there by linking people with different backgrounds. This paper analyzed the various type of the most popular social networking sites that are currently in used, the type of crimes that can be committed against students using social networking sites, the various ways that can be used to mitigate the activities of criminals, against the students, with the intention to apprehend them and to prove that the crime has actually been committed using the various forensic tools and techniques available. Modern day technologies provide a means by which criminal evade investigation and subsequent prosecution [25]. Various forensic science methods and techniques, that are used to investigate and recover digital information found on digital devices at crime/incident scenes are also explained [26].

2 LITERATURE REVIEW
With the primary used of Social networking sites for communication, business, e-commerce etc which makes it open for criminal elements to conduct crimes ranging from fraud, phishing, child pornography etc to use the services provided by Social networking sites to register themselves anonymously using fake identification to extract data from unsuspecting students like call history, mails, pictures, videos, Short Message Service (SMS), Multimedia Messaging Service (MMS), browsing history [7]. To conduct incidence investigation, to find out whether a crime has been committed against students, various forms of information in social networking sites like location information, user’s conversation,
personal network details, user friend list which are saved on a device synchronously can be collected using digital forensic and analyzed [6]. This means the necessary information required to conduct investigation has to be obtained which may reside on either the computer system or in the cloud as in the case of local computers and mobile devices respectfully. This local social networking sites information that is usually saved in form of artifacts can be used as evidence against a criminal to establish the existence of crime against students. The artefacts that are saved in the device of the suspect on some popular social networking sites of the students profiles in the dead analysis of the suspect's hard disk was carried out with respect to Yahoo Messenger [8], MSN Messenger, MSN/Windows Messenger[9], AOL Instant Messenger [11], Trillian basic [12], Windows Live Messenger, Pidgin Messenger [14], QQ [15], Skype [16], AIM Express, Google Talk, Meebo, E-buddy, IMs ([10], [13], [17]) using various methods and techniques to retrieve the data saved in the Social networking sites artefacts. The large number of social networking sites that are in existence today pose a serious threat to privacy and security of individuals [32], government agencies [33], cooperate organizations as well as students [33] due to the large amount of data that is being accumulated and saved in both the students and the social networking sites [34] servers which has to be analyzed forensically to detect, prevent or to prosecute the culprits [18].

3 SOCIAL NETWORKING SITES

The existence of social networking sites and the number of students that visits each of these sites every day poses serious threat to the security of our students, government agencies and corporate organizations and that means huge amount of data is being accumulated that is being used to commit crimes against our students. Even though so many countries use different social networking sites the most widely used, with more than 25 million users, as listed by ([3], [4], [35]) include the following:

<table>
<thead>
<tr>
<th>S/No.</th>
<th>Social Network</th>
<th>S/No.</th>
<th>Social Network</th>
<th>S/No.</th>
<th>Social Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Facebook</td>
<td>11</td>
<td>WhatsApp</td>
<td>21</td>
<td>YouTube</td>
</tr>
<tr>
<td>2</td>
<td>WeChat</td>
<td>12</td>
<td>QZone</td>
<td>22</td>
<td>QQ</td>
</tr>
<tr>
<td>3</td>
<td>Instagram</td>
<td>13</td>
<td>Twitter</td>
<td>23</td>
<td>Tumblr</td>
</tr>
<tr>
<td>4</td>
<td>Baidu Tieba</td>
<td>14</td>
<td>Skype</td>
<td>24</td>
<td>Google+</td>
</tr>
<tr>
<td>5</td>
<td>Sina Webo</td>
<td>15</td>
<td>LINE</td>
<td>25</td>
<td>Snapchat</td>
</tr>
<tr>
<td>6</td>
<td>YY</td>
<td>16</td>
<td>VKontakte (VK)</td>
<td>26</td>
<td>Viber</td>
</tr>
<tr>
<td>7</td>
<td>LinkedIn</td>
<td>17</td>
<td>Telegram</td>
<td>27</td>
<td>Pintrest</td>
</tr>
<tr>
<td>8</td>
<td>StumbleUpon</td>
<td>18</td>
<td>Foursquare</td>
<td>28</td>
<td>Reddit</td>
</tr>
<tr>
<td>9</td>
<td>Tagged</td>
<td>19</td>
<td>Badoo</td>
<td>29</td>
<td>Renren</td>
</tr>
<tr>
<td>10</td>
<td>MySpace</td>
<td>20</td>
<td>TheDots</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 TYPE OF CRIMES THAT CAN BE COMMITTED AGAINST STUDENT ON SOCIAL NETWORKING SITES

The following crimes can be considered as cybercrime that can be committed to students, in the course of their educational pursuits, by the use of social network as stated by ([18], [23], [24], [36]).

1 Credit Card Cracking: In which students are asked to offer their credit card or bank account details in exchange for money on the social networking sites during educational activities.

2 Credit Card Fraud: Fraudsers can collect students name, date of birth, and possibly the student bank address which they can be used to steal from the students’ social networking sites profile if the students account username and password is not well protected. The scammers used to pretend that they are their bank, the method that they use to collect students’ relevant information;
Nigerian Letter Fraud: Students are being tricked by sending a letter as an attachment through social networking sites convincing them to release some amount of money with a pledge to offer him/her a bigger sum as a gain;

Phishing: Falsely sending email to students pretending to be a legitimate enterprise thereby making the student to submit relevant private information to be used for the purchase of goods and services in respect of the student’s name by using e-mail; address posted on the student profile page on the social networking sites;

Spoofing: Obtaining sequence of keys strokes in order get student bank credentials by the use of malicious software e.g. malware in the student profile of the social networking site;

Luring young students to be the kidnapped by the use of Internet chatting in social networking sites;

Dissemination of abuse materials to students by using social networking sites;

Examination of the students social networking sites activities;

Deleted data recovery of student social networking sites;

Using social networking site to upload inappropriate pornographic films for downloading by students.

Spam: This is a technique used by cybercriminal to gather student personal data by persuading the student to share their personal information on the social networking site by promising them entertainment, competitions or other financial inducements [37];

Identity Theft: This is a situation where by a criminal would pretends to be an authorized user (malicious) so that he or she would be granted access to the relevant information on the social networking site by the student [38].

5 CYBERCRIMES DETECTION MEASURES AGAINST STUDENTS SOCIAL NETWORKING SITES

In order to conduct an investigation on social networking sites data in student conversations, profiles, friend list, personal relationships, local information are used in converting crime and useful for investigation using a digital forensic method [6]. ([12], [19], [20], [21], [22]) Identified the following methods, tools and applications for the conduct of forensic analysis to determine the possibility of crime against the students.

<table>
<thead>
<tr>
<th>S/No.</th>
<th>Forensic Techniques</th>
<th>Forensic Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Email Analysis</td>
<td>Cybercriminal used to alter the header of e-mails to make it look like it comes from a genuine source thereby misguiding students to open such mails which once open can steal the student relevant information from the social networking sites. Tools used to analyze students mails include MailXaminer, Aid4Mail, Digital Forensic Frame Work (DFF), eMailTrackerPro, Praben EMX, MX Toolbox, EmailTracer</td>
</tr>
<tr>
<td>2</td>
<td>File Viewers</td>
<td>As the cybercriminal engaged in their nefarious act they also try to save the collected data in to different file formats so that make it difficult for the students as they explore the social networking sites as well as the investigators to detect any criminal activity. File viewers are tools used to view those type files that are in different format and to save or export them in different format like bkf files, Lotus Notes DXL, E01 files within EDB, PST and OST, MDF, MSG, OLM, PPT, Visio diagrams and multimedia like DVD, audio CD VCD</td>
</tr>
<tr>
<td>3</td>
<td>File and Data Analysis</td>
<td>Files of different formats are collected and stored in database as the students are engaged in social networking sites in which forensic techniques are used to analyze such files to determine the possible of cybercrime against the students [41]. Some of the tools and techniques involve include: Prefetch analyser, DCode, Defraser, Forensic Image Viewer</td>
</tr>
</tbody>
</table>
4 Application Analysis
This is the process where vulnerability in software is tested before it is put into use thereby protecting the students social networking sites information against cybercriminals. Some of the common methods used include: Decrypts Dropbox file cache, download surrounding tiles using z,y,z coordinates in tiled filename, export and view Windows Live Messenger contact, view Skype chats and calls etc eg SkypeLogView, Google Maps Tile Investigator, LiveContactsView

5 Registry Analysis
The registry is a reserve for information that can be used by both the administrators and the forensic expert to find incidences of the software used by criminals against the students on social networking sites. Some of the tools used include Windows Registry Recovery, USB Device, ForensicUserInfo, Registry Decoder, RegEdt32, RegEdit

6 Internet Analysis
Used to capture students social networking sites browsing history in major browsers like Firefox, Chrome, Internet Explorer, Edge, offline parsing of session, reads cache folder, extract embedded data in Google Analytics cookies, stored password, captures information from social media profiles like Facebook, reads and parses cookie folder in browsers, reads queries pass to search engines and social networking sites

7 MAC OS Analysis
This is used to conduct forensic analysis of social networking sites on MAC Operating System for those students who possess MAC devices. They are specifically used to perform the following operations: blocking of file system mounting, complementing write blocker to disable disk arbitration, converts times, obtain the list of devices that is connected to the computer system, partition information, size, bus and types that is connects the device, Conduct Memory Forensic, eg Audit, Disk Arbitrator, Epoch Converter, IORegInfo

8 Mobile Device Analysis
On social networking sites, presently, students mostly use mobile devices to interact with one another. Therefore, there is the need for a cross-platform tools that would enable us to conduct mobile forensic on the students’ mobile devices. These tools are used to perform forensic analysis like exploring backups, internal file structures of mobile devices, extraction of mobile devices model and software versions and date of creation including GPS data from mobile videos, get messages, call logs and contacts eg SAFT, ivMeta, IPBA2, iPhone Analyser

9 Network Forensics
Used to capture and analyze social networking sites events and how cybercrime against students can be detected and prevented. It comprises of the following forensic activities Email forensic, Web forensic, packet snippers, IP traceback techniques, Honeyports, Honeynets at the same time the following set of tools are being used like EmailTrackerPro, SmartWholes, WebHistorian, Inde.dat analyzer, Ethereal, WinPcap, AirPcap, Control Flooding, Input Debugging, Packet Marking Techniques, ICMP Traceback, Source Path Isolation Engine, Serial vs Parallel Architecture, Virtual Honeypots

6 CYBERCRIMES PREVENTION MEASURES AGAINST STUDENTS SOCIAL NETWORKING SITES
For the prevention of cybercrime against students many measures including the use of social networking sites software can be adopted. Some of the major tools that are used to provide prevention against such crimes include the following:

6.1 Social Networking Sites Crime Controls Measures
According to ([28], [29], [30]) there are tools and methods that can be used by parents, administrators and teachers on how to monitor and control the students’ use of social networking sites. Some of the common activities that can be performed using these tools include:

a) Monitor Students call logs and locations tracking on social networking sites;
b) Setting students social networking sites to invisible mode, remote activity view;
c) Prevention of students against social networking sites cyber predators;
d) Prevention of students against online bullies and data breaches on social networking sites;
e) Spying on the students social networking sites chats and also read their conversation;
f) Spying on students social networking sites video and audio conversations;
g) Hack students social networking sites chat screen to monitor and record back to back video of the students’ mobile device;
h) All sent and received students’ photos and other media can be tracked on social networking sites;

i) The timestamp of all students’ social networking sites activities can be tracked;

j) The metadata of all file types can be read, written and edited to extract relevant information from devices of the students used on social networking sites;

k) Detection and prevention of hate speech between students using social networking sites.

6.2 Social Networking Sites Crime Controls Tools

According to [29] the motivation for using social networking sites by students are the provision of efficient and quick method of communication, sharing of documents, saving time, helps in better students'/teacher interaction, students collaboration in the class, experimenting with improved tools and techniques. Some social networking sites make provision for parental controls while some have the capability to monitor students’ location, what they post or posted to them, capture each picture posted on profiles directly [29]. In that regards [30] identified the following Facebook parental control tools for both parents and teachers to control how the students use the social networking sites. These tools include Spyzie, SecureTeen, Norton Family Premier, Net Nanny Social, Familoop Safeguard, Bitdefender, Puresight Owl, Safe eyes, SniperSpy, QuStudio, in addition, TheOneSpy, provides enhance monitoring of students by providing additional features [31] such as monitoring of Whatsapp, Instagram, Windows, Android, Mac OS, iPhone, Snapchat, Line as well as tracking of chatting in Facebook, Viber, Skype etc.

7 CONCLUSION

With the advancement in the way Social networking sites allow students to communicate and share data and information among different groups of students as well as their teachers and the sophistication by which crimes are also committed, there exist also a lot of technologies and tools and can be used to monitor, track and apprehend the criminals that are using Social networking sites to commit crimes against students. Forensic science provides a lot of tools and technologies to prove whether a crime has actually been committed so as to protect our students against the menace of social networking sites.

REFERENCES


