Society & Change
Vol. VI, No. 3, July-September 2012
ISSN :1997-1052 (Print), 227-202X (Online)

Innocent Victimization of Cyber and Social Networking Crime: An Empirical Assessment among the Graduate Students of Tangail.

Mohammad Ashraful Alam[1]
Amit Sarker[2]
Dr. Md. Jahangir Alam[3]

Abstract

Social Networking means to bring the world closer, foster unity and make us all part of happy social village. With the tide of recent times, the Facebook, MySpace, LinkedIn, Twitter, Ning, Digg, MeetUp, blogs, etc., have become a hotbed for online criminals because of their global reach and the participation by hundreds of millions of active users from all walks of life. The present study voyages through discovering dimensional orientations and impishness of cybercrime in social networking in student life. Purposive sampling method was used for selecting study area and as well as respondents within the study areas. About 121 respondents were taken for the intended study. The study has identified the practical strategy of Social Networking crime among respondents; dimensions of criminalization & behavioral orientation of cyber offenders on their target. Also has determined the aspects & impacts of victimization and sufferings of the respondents in real life context. Variation in offending & victimizing found in terms of geographical location, age, religion, gender, and monthly income of family members. Factors of counter measures for defending cybercrimes on Social Networking crime should needed to be some security measures to reduce the possible victimization and also have to improve the efficient and better safely in online communication & sharing on Social Networking Sites.

Keywords: Cyber Crime, Social Networking Crime, Innocent Victimization, Users Identity, False Identity, Image Manipulation, Cyber Stalking.

[1] Assistant Professor Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Tangail.
[2] B. Sc. (Hons) in Criminology and Police Science, Mawlana Bhashani Science and Technology University, Tangail.
[3] Associate Professor, Department of Sociology, University of Dhaka.

Introduction

Social networking is everywhere and common to find parents, children, friends, co-workers and even the elderly on the networks across the social media world on various sites such as Twitter, MySpace, Facebook, YouTube and LinkedIn, etc. These days nearly everyone belongs to a social network, where they spend time from one to several hours per day, posting photos, instant messaging, tweeting, and posting their locations on Facebook and any other number of windows into personal daily lives. While social networking has become a staple of social interaction, therein lays a great deal of potential dangers. Social networking has opened up many new doorways for cyber-crime, and with all the people on social networks who are completely new to technology, it is more important than ever to make sure people are aware of the risks. One of the worst things about the crimes committed through social networking sites is that just about anyone is at risk, no matter who they are. Anyone from a CFO (Chief Financial Officer) of a major credit union to a 14 year old girl, or a new college graduate to a retired senior citizen, is a potential for those that hunt out and prey upon unsuspecting social network users. The criminals, who target people for personal information, passwords, pass codes and other sensitive information, are extremely skilled at what they do. They can con reasonable people into giving up information, and steal valuable secrets, all without the victim even being aware a crime was committed at all. (Melissa, 2011)

Social Networking

Social Networking, It's the way the 21st century communicates today. Web 2.0 opportunity comes through social networking sites like MySpace, Facebook, Twitter, YouTube and LinkedIn. These sites allow their users to interact with each other in many ways, either by sharing pictures, joining groups, sending private messages, and using other constantly-evolving applications. Social networking websites function like an online community of internet users. Social networking often involves grouping specific individuals or organizations together. While there are a number of social networking websites that focus on particular interests, there are others that do not. The websites without a main focus are often referred to as "traditional" social networking websites and usually have open memberships. This means that anyone can become a member, no matter what their hobbies, beliefs, or views are. However, once any one inside this online community, he/she can begin to create his/ her own network of friends and eliminate members that do not share common interests or goals.(www.whatissocialnetworking.com, 2011).

The Wave of Social Networking & Innovation of Crime

Historically, long before it became the commercialized mass information and entertainment juggernaut it is today, long before it was accessible to the general public. In the 1970s that process began in earnest. (Christopher Nickson, 2009). It started with the BBS (Bulletin Board System)**.** Short for Bulletin Board System, these online meeting places were effectively independently produced hunks of code that allowed users to communicate with a central system where they could download files or games (many times including pirated software) and post messages to other users. Accessed over telephone lines via a modem, BBS's were often run by hobbyists who carefully nurtured the social aspects and interest-specific nature of their projects. There were also other avenues for social interaction long before the Internet exploded onto the mainstream consciousness. One such option was CompuServe, a service that began life in the 1970s as a business-oriented mainframe computer communication solution, but expanded into the public domain in the late 1980s.CompuServe allowed members to share files and access news and events. But it also offered something few had ever experienced – true interaction. But if there is a true precursor to today's social networking sites, it was likely spawned under the AOL (America Online) umbrella. In many ways, and for many people, AOL was the Internet before the Internet, and its member-created communities (complete with searchable "Member Profiles," in which users would list pertinent details about themselves), were arguably the service's most fascinating, forward-thinking feature. (Christopher Nickson, 2009). Yet there was no stopping the real Internet, and by the mid-1990s it was moving full bore. Yahoo had just set up shop, Amazon had just begun selling books, and the race to get a PC in every household was on. And, by 1995, the site that may have been the first to fulfill the modern definition of social networking was born. That same level of success can't be said for SixDegrees.com. Sporting a name based on the theory somehow associated with actor Kevin Bacon that no person is separated by more than six degrees from another, the site sprung up in 1997 and was one of the very first to allow its users to create profiles, invite friends, organize groups, and surf other user profiles. Its founders worked the six degrees angle hard by encouraging members to bring more people into the fold. Unfortunately, this "encouragement" ultimately became a bit too pushy for many, and the site slowly de-evolved into a loose association of computer users and numerous complaints of spam-filled membership drives. SixDegrees.com folded completely just after the turn of the millennium. (Christopher Nickson, 2009). Other sites of the era opted solely for niche, demographic-driven markets. One was AsianAvenue.com, founded in

1997. A product of Community Connect Inc., which itself was founded just one year prior in the New York apartment of former investment banker and future Community Connect CEO Ben Sun, AsianAvenue.com was followed in 1999 by BlackPlanet.com, and in 2000 by the Hispanic-oriented MiGente.com. All three have survived to this very day, with BlackPlanet.com in particular enjoying tremendous success throughout its run. (Christopher Nickson, 2009). In 2002, social networking hit really its stride with the launch of Friendster. Friendster used a degree of separation concept similar to that of the now-defunct SixDegrees.com, refined it into a routine dubbed the "Circle of Friends" (wherein the pathways connecting two people are displayed). (Christopher Nickson, 2009). Introduced just a year later in 2003, LinkedIn took a decidedly more serious, sober approach to the social networking phenomenon. Rather than being a mere playground for former classmates, teenagers, and cyberspace Don Juans, LinkedIn was, and still is, a networking resource for businesspeople who want to connect with other professionals. In fact, LinkedIn contacts are referred to as "connections." Today, LinkedIn boasts more than 30 million members. (Christopher Nickson, 2009).

More than tripling that number, according to recent estimates, is MySpace, also launched in 2003. Though it no longer resides upon the social networking throne in many English-speaking countries – that honor now belongs to Facebook (Garry Barker, 2010). YouTube in all the countries over the globe – MySpace remains the perennial favorite in the USA. It does so by tempting the key young adult demographic with music, music videos, and a funky, feature-filled environment. It looked and felt hipper than major competitor Friendster right from the start, and it conducted a campaign of sorts in the early days to show alienated Friendster users just what they were missing (Wikipedia, 2011). It is, however, the ubiquitous Facebook that now leads the global social networking pack. Founded, like many social networking sites, by university students who initially peddled their product to other university students, Facebook launched in 2004 as a Harvard-only exercise and remained a campus-oriented site for two full years before finally opening to the general public in 2006. Yet even by that time, Facebook was seriously big business. The secret of Facebook’s success (it now currently boasts in excess of 800 million users) is a subject of some debate. With over 800 million users, Facebook is now used by 1 in every 13 people on earth, with over 250 million of them (over 50%) who log in every day. The average user still has about 130 friends, but that should expand in 2012. Some point to its ease of use, others to its multitude of easily-accessed features, and still others to a far simpler factor – its memorable, descriptive name. A highly targeted advertising model certainly hasn’t

hurt, nor did financial injections. Regardless, there's agreement on one thing – Facebook promotes both honesty and openness. It seems people really enjoy being themselves, and throwing that openness out there for all to see (http://www. facebook.com/ press/info.php/statistics; 2011).

Let's focus at Twitter. Essentially a micro-blogging "What are you doing at the moment?" site where users keep contacts informed of everyday events through bite-size morsels they post from their computer or handheld device, the service got off to a very good start when launched in 2006. Its continued popularity notwithstanding, Twitter has nevertheless come under some criticism for taking the "staying in touch" thing too far. (Christopher Nickson, 2009). Twitter semi-clone Jaiku, despite a promising debut in 2006 and a Google buyout the following year, has already U-turned in the wrong direction with the January 2009 announcement that Google is cutting support for the service. Only time will tell- how heavily will the current economic crisis and the decreasing ad revenue it generates negatively impact social networking goliaths such as Facebook, MySpace, and LinkedIn? Still, one thing's for certain – for the present at least, going forward, we'll all be certain to read about the field's continuing development one status update at a time (Christopher Nickson, 2009).

Online Crime Innovation and Rise of Social Networks

Social networking websites have become a hotbed for online criminals because of their global reach and the participation by hundreds of millions of active users from all walks of life. This makes these communities prime targets for exploitation by criminals who seek to steal personal information through socially engineered attacks. Reflective of this trend, the survey exposed that four out of five people using social networking websites displayed concern with the safety of their personal information online (Egov Asia Editors, 2010). These online criminals are adept at social engineering with at-the-ready phishing attacks that are launched within moments of breaking news about popular celebrities, professional athletes or serious global events. In these cases, people are lured to legitimate websites infected with malware as well as complete fakes designed to look like well-known news sources."Security is a constant arms race," said Simon Axten (2010) - an associate for privacy and public policy at Facebook. Additionally, "Malicious actors are constantly attacking the site, and what you see is actually a very small percentage of what's attempted" (EgovAsia Editors, 2010).

Vulnerable Contextual Orientation of Present Reality

Experts say cyber crooks are lurking just a mouse click away on popular social networking sites. That's because more cyber thieves are targeting

increasingly popular social networking sites that provide a gold mine of personal information, according to the FBI. Since 2006, nearly 3,200 account hijacking cases have been reported to the Internet Crime Complaint Center, a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance (Stephanie Chen, 2009). When the message or link is opened, social network users are lured to fake Web sites that trick them into divulging personal details and passwords. The process, known as a phishing attack or malware, can infiltrate users' accounts without their consent. Once the account is compromised, the thieves can infiltrate the list of friends or contacts and repeat the attack on subsequent victims. Social networking sites show there is ample opportunity to find more victims; Scammers break into accounts posing as friends of users, sending spam that directs them to websites that steal personal information and spread viruses. Hackers tend to take control of infected PCs for identity theft, spamming and other nasty mischief's such as blackmailing, pornography etc. (Information provided by FBI and Internet security experts, 2011).

In this vulnerable reality context, in here, at Bangladesh the several social networking media have already earn enormous popularity in all spares of citizen life. It's have been one of the daily life accessories of modern life- especially for youth it almost true that they are in the mode of silent fever of social networking media especially for Facebook, YouTube and twitter etc. Actually they feel a strong affinity regarding this web; it is difficult to find any one; who have the internet connection but no account either in Facebook, twitter or YouTube. But the problem is most of all here have very little concept about cyber world i.e. the dangerous loopholes of the virtual world. So sometimes this, too much unawareness causes too much vulnerability and unexpected danger beyond their senses. In our prevailing socio-economic aspects the sufferings have deep impact for female than male. In our country, yet we are not in that stage of implementing the cyber law and regulation to detecting and apprehending the all of these criminals in time. Most of the case, the victims are not willing to report these occurrence due to social and complex legal proceedings.

Review of Literature

Boyd and Ellison (2007) In their in-depth review of scholarship on social network sites, Boyd and Ellison (2007) noted that "the bulk of SNS research has focused on impression management and friendship performance, networks and network structure, [bridging] online [and] offline connections, and privacy issues" (p. 219). Of concern here is the potential of SNS to bridge (or create a gap) between online and offline connections, a key component of social capital theory. "Facebook is the

social network du jour. Attackers go where the people go. Always," said Mary Landesman, a senior researcher at Web security company Scan Safe (Mary Landesman, Web security company ScanSafe, 2011). Facebook manages security from its central headquarters in Palo Alto, California, screening out much of the spam and malicious software targeting its users. That should make it a safer place to surf than the broader Internet, but criminals are relentless and some break through Facebook's considerable filter. The rises in attacks reflect Facebook's massive growth. Company spokesman Simon Axten said that as the number of users has increased; the percentage of successful attacks has stayed about the same, remaining at less than 1 percent of members over the past five years (Simon Axten, Company spokesman- Facebook, 2011).

The growth in social networking and the implicit trust in these communities have given rise to new threat vectors in places like Facebook, Twitter and YouTube. Facebook and other social networking sites do not vet the community's shared programs for security issues, while Twitter and others have been plagued by a number of issues. Within these communities, threats now travel faster due to the enormous amount of trust their users place in one another. Because these web 2.0 generation of applications and websites provide enormous value to their user base, it is important to embrace them while also determining the best way to ensure these communities improve their safety for online users, and that the users themselves understand the implications. As when societies begin relying upon email in earnest, and virus education began in earnest, a similar urgent level of education is necessary for the use of web 2.0 (McAffee- Leading American based internet security Software Corporation, 2010). Another report McAfee, the world's No. 2 security software maker, says Koobface variants almost quadrupled last month to 4,000. "Because Facebook is a closed system, we have a tremendous advantage over e-mail. Once we detect a spam message, we can delete that message in all inboxes across the site," (Craig Schmugar, McAfee Inc MFE.N researcher, 2011).

Cybercrime is rapidly spreading on Facebook as fraudsters prey on users who think the world's top social networking site is a safe haven on the Internet. News Corp's (NWSA.O) MySpace was the most-popular hangout for cyber criminals two years ago, experts say hackers are now entrenched on Facebook, whose membership has soared from 120 million in December to more than 200 million today. Scammers break into accounts posing as friends of users, sending spam that directs them to websites that steal personal information and spread viruses. Hackers tend

to take control of infected PCs for identity theft, spamming and other mischief (Jim Finkle, 2009). According to Priyankan Goswami 'Exploitations in Facebook and cybercrime- Growth of a social curse' that the curse of Social Media is not just limited to reputation threats. It has damaged human relations even more. Wedding invitations and even baby shower invites are sent out nowadays by creating events! Fake profiles, cyber criminals, video blackmailers and your unknown friends whom you added as friend in Facebook because he or she looked nice, are all out to destroy your social reputation forever. The result, – the charm of being in Facebook and liking someone's comments and pictures is slowly evading. It comes with a heavy cost, – a threat to wipe your social status completely. It happened in Orkut before, but with Facebook it's more costly since the Media is at watch in Facebook and Media just loves juicy stories! (Goswami, 2011). Samanth Murphy said in 'Facebook Crimes on the Rise, Experts Warn' article that social media website rely on carefully crafted baits that often include scandalous and explicit video content or exclusive footage of the latest and hottest events, from celebrity death claims to never-before-seen footage of a natural disaster. Meanwhile, rarer cybercrimes on Facebook involve the installation of malicious software, or "malware," on computers so credit card information can be easily stolen. However, the rise of these Facebook crimes isn't limited to just scams and phishing activities. There's also cyber bullying, sexual predation and even robberies that occur after users post GPS location about their whereabouts to inform others they are out of town (Samanth Murphy, 2011). Rajeev Saxena expressed in Facebook Now Marred by Cybercrime report that the bane of all internet users, Cybercrime, is fast spreading itself in the realms of one of the most secured social networking websites, Facebook. According to recent reports, hackers and other online menaces have been taking over various Facebook accounts and creating havoc over the web (Rajeev Saxena, 2009). Michelle Kessler, USA noted in 'Facebook users under cyber-attack' that two top botnet gangs are bombarding Facebook members with targeted phishing emails. They're hoping to get control of members' Facebook and other accounts (Michelle Kessler, USA, 2009). The CNN reports about 'Facebook, Twitter users beware, Crooks area mouse click away' opinion that cyber thieves are targeting increasingly popular social networking sites that provide a gold mine of personal information, according to the FBI. Since 2006, nearly 3,200 account hijacking cases have been reported to the Internet Crime Complaint Center, a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance. Some social networking sites experience monstrous growth, they are becoming a new and extremely lucrative - frontier for cybercrime. Early this year, Twitter experienced several phishing attacks

in which a Web page that looked identical to the widely recognized light blue Twitter page was a hoax. The company warned users to double-check the URL to ensure they were visiting the correct site. The Internet Crime Complaint Center received more than 72,000 complaints about Internet fraud in 2008 that were referred to law enforcement agencies for further investigation. These cases involved financial losses amounting to $264.6 million, an increase from 2007. Each person lost an average of $931 (Stephanie Chen, 2009). The Web security firm SOPHOS Social networking websites such as Facebook, Twitter and MySpace will soon become the most insidious places on the Internet, where users are most likely to face cyber-attacks and digital annoyances (Sophos Security Threat Report Jul, 2009) and Sophos in a recent report surveyed 1200 computer users in December, 2010 and revealed spam has increased by 10% from December 2009 to December 2010; phishing has increased from 30% to 43% during the same period and malware threat grew marginally from 36% to 40% (Tanuj Lakhina, 2011). According to the UK Police, Facebook crime also rose by 540 percent in 3 years. In the period of 2005 till 2010, London police had received 100,000 crimes linked to Facebook while 2010 alone contributed to 7,545 calls.While revealing too much information on profiles and updates is an issue, checking-in via Foursquare or Facebook Places can be a big invitation to home invasions/thefts/burglary, mugging, sexual predators and/or kidnapping. In a study Mr. Barrett shows that one in four users of social networking sites unwittingly leave themselves open to crime by revealing personal details, it was claimed today. Government-backed research for the Get Safe Online week found 25% of the 10.8 million Britons registered with networking websites expose information such as contact details or dates of birth on their online “profiles". Among 18 to 24-year-olds the proportion putting them at risk of identity fraud rises to 34%. The survey showed 13% of social networkers had posted information or photos about other people without their consent, rising to 27% of 18 to 24s. The poll also found 15% of people do not use any privacy settings on social networking sites, and almost one in four (24%) people use the same password for all websites (David Barrett, 2007).

From the work of Portland University shows Facebook is still the most common place that web users are targeted by cybercrime. Officials from CommTouch, who authored the report, said that this may be because the website fosters personal connections, which makes some users unaware that they may be targeted by criminals. Additionally, the report states that the use of malware, or malicious software, on Facebook has also grown. This year, the researchers found that one of the most common techniques for spreading malware was through a program that promised Facebook

users that they could see who was viewing their profile if they clicked on a link. Another scam that cyber criminals used this year was sending Facebook users messages that said their accounts were shut down and prompting them to click on a link in order to revive their pages, e-Week reports. When people do so, the link downloads a virtual worm on their computers, which essentially hijacks their Facebook accounts (Portland State University, 2011). The Hindu of India news claims, Facebook crimes on the rise, say experts express that - Facebook crimes such as scams, bullying, phishing and many other forms of illegal activities, are soaring and are getting more sophisticated, cyber experts have warned. Rarer cybercrimes on Facebook involve the installation of malicious software or 'malware' on computers so credit card information can be easily stolen (The Hindu, 24 September, 2011). Experts' claim that the crimes are not limited to just scams and phishing, there are sexual predators that use this forum, and even robberies have been reported when users post the GPS location to inform others about their whereabouts when out of town. According to Paul Zak (2011), a professor at Claremont College in southern California, scammers prey on Facebook because they don't know their victims, the report said. "It is easier to hurt someone when you're not seeing them in person." "Neuroscience research shows that moral violations are less likely when interactions are personal because people empathize with those they meet in person. In the online world, people are just a number," he added. According to Ioana Jelea (2011), communication specialist at Bit Defender, the social scam industry is thriving because scam creators are taking legitimate Facebook functionalities and persuading people to click on links. Ms. Jelea also argued that it's not just users' trust in the platform that puts them at risk, but also their insufficient familiarity with Facebook's security and privacy settings (The Hindu, 24 September, 2011). Kevin Voigt shows (2009), Twitter message could be cyber-criminal at work express that Cyber criminals are setting snares that move at the speed of news."Cyber criminals have been targeting Twitter users by creating thousands of messages (tweets) embedded with words involving trending topics and malicious URLs," Sean-Paul Correll (2009), a threat researcher for Panda Labs, wrote recently on a blog for the company (Kevin Voigt of CNN, June 21, 2009). The Times of India**,** reports that Social networking sites have become hunting ground for cyber criminals. Complaints related to morphing of photographs on somebody's profile, credit card frauds, fake profiling, defamation on the internet, and black dollar and lottery scams are common. Officials say young people, executives in private companies and students usually become victims of crimes like fake profiling and hacking of emails. According to Delhi Police's official figures , there were 113 complaints of

intimidation by unknown and known persons on the internet ; 282 complaints of hacking of emails or identity thefts on social networking sites; and 75 complaints of posting of fake profiles on Facebook and Orkut. In addition, there were 184 complaints of credit card frauds; 509 complaints of black dollar and lottery scams (where Nigerian nationals usually promise to pay huge sums of money through email); and 105 complaints of defamation (when somebody writes abusive or obscene things on somebody's profile). There were 208 miscellaneous complaints as well in which people reported several other crimes on the internet (Neeraj Chauhan, February 12, 2011).

Some features of Social Networking Statistics

15% of Americans have never checked their social networking privacy and security account settings (National Cyber Security Alliance (NCSA)-MacAfee Online Safety Study, 2011). 41% of social media-using teens have experienced at least one negative outcome as a result of using a social networking site (Pew Research Center, FOSI, Cable in the Classroom, 2011). 29% of Internet sex crime relationships were initiated on a social networking site (Journal of Adolescent Health 27, 2010). In 26% of online sex crimes against minors, offenders disseminated information and/or pictures of the victim through the victim's personal social networking site (Journal of Adolescent Health 47, 2010). 33% of all Internet-initiated sex crimes involved social networking sites (Journal of Adolescent Health 47, 2010). 24% of Americans say they are not at all confident in their ability to use privacy settings (National Cyber Security Alliance (NCSA) - MacAfee Online Safety Study, 2011). In half of all sex crimes against a minor involving a social networking site, the social networking site was used to initiate the relationship. (Journal of Adolescent Health 47, 2010). Of the active adult users of Facebook, 66% reported they did not know privacy controls existed on Facebook and/or they did not know how to use the privacy controls. (Consumer Reports, June 2011). 29% of Internet sex crime relationships were initiated on a social networking site (Journal of Adolescent Health 47, 2010). 72% of teens have a social networking profile and nearly half (47%) have a public profile viewable by anyone. (Teen Online & Wireless Safety Survey: Cyber bullying, Sexting and Parental Controls: Cox Communications Teen Online and Wireless Safety Survey in Partnership with the National Center for Missing and Exploited Children, 2009: Cox Communications Teen Internet Safety Survey, Wave II, 2007). 59% of teens perceive that public blogs or social networking sites are unsafe (Teen Online & Wireless Safety Survey: Cyber bullying, Sexting and Parental Controls: Cox Communications Teen Online and Wireless

Safety Survey in Partnership with the National Center for Missing and Exploited Children, 2009). 76% of teens are at least somewhat concerned that posting information publicly could negatively impact future.(Teen Online & Wireless Safety Survey: Cyber bullying, Sexting and Parental Controls: Cox Communications Teen Online and Wireless Safety Survey in Partnership with the National Center for Missing and Exploited Children, 2009). According to online & wireless safety survey (2009) 26% of teens know someone something bad has happened to because of information or photos posted online Teen (www.internetsafety101.org, 2011).

Exploring the Buzzers Social Networking Based crimes among Students

The present world prevails in rampant era of the science and technology. With the boost of globalization and other creative blessings of science, the information technology have get new wind on its vast sail to wing through all over the globe. The social networking media especially the Facebook, Twitter, YouTube and MySpace etc. have already become recognized as some of the greatest strategy of the development of science and technology, but also our modern enlightened daily life. There is another truth that since there have been human presence in the earth, there also been the presence of deviancy/crimes in this earth. In another simple languages, there have always been criminals and victims presence in this earth; as the time changes the mode, patterns, effects, impact changes for both the regard. In the road of this way, cybercrime has come as the most complicated and daring devil form of crimes in this modern technology era. The cybercrime/deviancy via social networking media can recognize as most vulnerable and widespread modern life problem of the every corner of the world. It is the significant matter to focus that this notorious acts has not been committed by any illiterate or poor person, rather, it has become the acts of well-educated in must be with science or technology, mostly well financed peoples, especially among the youth generation in various ways by using computer or high quality and latest mobile phones. So it can easily assumed that most of the occurrence this patterns of crime fully relay upon to the gentle educated man. Actually influences of these patterns of cybercrime depend on several aspects i.e. The base factors of the crimes are morality devaluation, bad peer effects, cultural deviation, personal disorder etc. I belief all the man have experienced on his/her different learning stages of human life. The computer and internet has recognized as obvious learning materials in higher and supreme academic learning strategies of modern creative world. In this real context at here, as a student of Criminology and Police Science Department, I have rational interest to find out the actual specific situation of Mawlana Bhashani Science and Technology University as

because not only it is a technology based university but also the English medium modern learning system. The computer has become one of the indispensible parts of academic learning process and like all and everywhere; the popularity of social networking media has gained very much popularity among the students. So I think is always a challenging and vital strategies upon me to find out the truth of this modern and youth attracting aspects cyber-crime and the silent effect upon the victims on both academic and social context.

Measuring the Orientations/Magnitudes

The social networking has become a dazzling phenomenon of youth and modern busy life in everywhere of the planet. Among the students, crimes invade here basically via two ways - Enlighten Accessories (e.g. Audio, Video, Image, text, Web-cam etc.) and users' personal information (e.g. fake profiling, phishing, cyber stalking, hacking~ cracking, illegal/ deviant group activities etc.). These procedures have become facilitated due to several reasons. Most important among them are- Lack of Cyber knowledge; Easy to access; Unawareness; Criminal mentality; Lack of protection/security etc. All these, causes and Medium/ procedures or mediums finally meet together on a focal point i.e. the event of innocent victimization of general users. Here, this isn't the ending of the victimization story; ironically it have been putting some vulnerable impacts upon the innocent victims such as Mental suspension, Social insecurities, Inferiority; Labeling, Helplessness etc.

Methodology:

This research based on assessment of Social Networking Media and Crime among the university students. The study was a cross-sectional survey indeed and quantitative in nature. Data were analyzed as well as interpreted for descriptive purpose. Data gathered from different students of different education levels. The students use computer and internet facilities as obvious educational tool for different academic and lifestyle purpose, also familiar with the different social networking media and its good & bad aspects. Their psychological and behavioral attributes mostly form and help to explore the actual image of different incidents of deviancy or crime in social networking media also the following consequence to victim.

Sampling &Data Collection:

For the intended study, Tangail district was selected as primary sampling unit as because there is several prominent educational institutes are situated where graduate level courses are available and also there have enough modern technological facilities for students. On the other side there was some opportunity to access both the primary sample and the

Secondary data because of the researchers' communication with students and teachers and also academic resources. In this regards, Mawlana Bhashani Science and Technology University were selected purposively as final sampling units. Students of all departments were selected for study population. Respondents were selected on the process of Purposive Sampling. The sample size was determined by using scientific formula based on non probability sampling method. For the study the sample size was 121 individual case of occurrence among the students. Data was collected from the student via structured and mixed questionnaire through direct face to face interview. The interview-schedule consists of three major sections. It is designed to secure information to explore the incidents which were proposed in the scheme. The first section deals with questions relating to the background of the respondents, i.e. factual information. The second section contains questions relating to their activities of on social networking world. The third section includes questions dealing with information to feelings about victimization incident and sufferings. It is designed in English. Respondents who were selected to response the causations noted in the questionnaire were asked the questions. The answers given by the respondent were noted in the interview-schedule and that was produced a dataset for the study.

Data Analysis:

Several levels of statistical analyses are performed in conducting analysis stage. Frequency tables, i.e. frequency distribution, central tendency was made for univariate analysis. Bivariate (correlation, lambda,) analyses are used to see the relation among the variables. Cross tabulation were obtained in terms of: age, gender, religion, category of user, sufferings experience on Social Networking Media (S.N.M), orientation of sufferings, academic impacts of sufferings, sufferings & suicide fake ID, misusing of fake account, preferable medium on misusing account, impact upon academic study, thinking about committing suicide, the liability of victimization, offenders aftermath assessments, etc., among the respondents.

Findings

Table-01: Exploring the Criminological Dimensions of Social Networking Based crimes among respondents

Characteristics \ Crime		Most Favorite Social Networking Media	Multiple Accounts Location	Offenders' Preferable Host Site for Misusing Account	Vulnerability on Social Networking Media[victim's Sense]
Social N. Hosts	Facebook	93.39%	87.69%	82.81%	96.34%
	Twitter	4.13%	7.69%	10.94%	2.44%
	You tube	2.48%	4.62%	6.25%	1.22%
	Total	**100%**	**100%**	**100%**	**100%**

Most Favorite Social Networking Media: The study revealed that among the students uses basically the Facebook, the Twitter & the YouTube on social networking and communicating purpose. But the strategy of Facebook is different here; as this social networking site already win most of the students heart. About 93.39% students have recognized The Facebook as their most favorite Social Networking Media. *Multiple Accounts Location:* On exploring the strategy, I get information that most of the case and most of the multiple accounts located on the social networking host the Facebook about 87.69%. So, we can assume the respondents, most of the case the cybercrimes are conducted upon Social Networking Site via the Facebook. *Offenders' Preferable Host Site for Misusing Account:* This study revealed that in most of the cases (82.81%); they like Facebook as the preferable host site i.e. Facebook accounts have been hugely misused by the respondents. It is as this because, most of the students having a Facebook account- at least, whom have an internet connection; besides many students whom haven't yet any own internet connection they also having at least a Facebook account & access it with the support of his/her friend's internet connection. So the criminals can easily choose their suitable targets among this huge availability of Facebook accounts. Moreover, Facebook is a multi-dimensional purposeful Social networking Site, where user can share text, image, audio, video and so on. So this site has very much attractive for both the general user and intending offenders.

The second preferable hosting site for misusing the account is YouTube; 10.94% only. Actually the YouTube is a mono dimensional site- there user can only share video formatted properties; so naturally YouTube oriented cyber-crimes have less proportionate than Facebook crimes. Another factor is the prevailing environment of the campus and local surroundings i.e. the over-all campus environment has yet been moderately conservative and slightly undeveloped than other prominent universities of the country. So offenders yet not fully capable of publishing video related (e.g. Pornography) nuisance on Social Networking sites, especially on YouTube. On regional real context as a social networking media site the Twitter, has yet not popular among the offenders also among students like Facebook and YouTube. It's also a mono dimensional social networking site. Also one can only commit certain types of wrong doings via Twitter & this has very little impact upon youth life (most of the cases); only 6.25% has been conducted via Twitter.*Vulnerability on Social Networking Media:* The victims of the

study have been victimized on three popular Social Networking Host Site; they are- The Facebook, the YouTube &the Twitter. The reality is most of the victims have become victimized on the most popular social Networking Host Site; the Facebook, about 96.34%. So the Facebook has become the most vulnerable Social Networking Media Host Site for the Victims. Simply it is as this because Most of the Social Networking Media user, Pay vital attention on Facebook i.e. if any one may talk about Social Networking Media; at first they think about the Facebook rather any other host site of Social Networking Media. More ever, only 2.44% students have been victimized via the YouTube &1.22% has been victimized on Twitter on cyber space of the Social Networking Media.

Table-02: Profile of Offenders' Activities through Social Networking Site

Age Group	**16-18 (3.3%)**	**19-21 (31.4%)**	**22-24 (52.9%)**	**25-27 (12.4%)**
Account Type	Single (43.3%)	Multiple (53.7%)		
Personal Experience to Misuse of Own Fake ID/ Multiple Accounts	Yes (98.64%)	No (1.54%)		
Preferable Medium/ Process of Misusing the Fake ID/ Account	Image (32.8%)	Video/Audio (10.9%)	Text (21.9%)	Personal Information (34.4%)
Misusing the Fake ID/ Accounts [Via Image/Video/Text/Audio]	Unauthorized Publishing on Others Account (45.24%)	Pornography Related Publishing (21.43%)	Threatening/ Slung Text Related (33.33%)	
Misusing the Fake ID/ Accounts [Via Personal Information]	Cyber Stalking (72.73%)	Black Mailing (13.64%)	Crackers own Property Hacking (13.64%)	
Offender's Aftermath Assessment / Feelings towards Victims	Don't Care (51.56%)	Nothing (35.94%)	Feel Guiltiness (12.5%)	

From table -02, Age Group: Among the respondent's all are youth-Adult. Most of the students are in the age group of 22-24 years, about 52.9%. The next large category consists of 31.4%of the age group of 19-21. *Account Type:* The present study represents that for most of the cases 53.7% having multiple accounts and rest of 46.7% having a necessary single account. In most of the cases these are the pupils whom involved in cybercrime on Social Networking Media via different (already opened these multiple Fake ID (Identity Theft). Additionally, the users are trends

to enhance and increase their pleasure and scope of the utility of social networking media via using multiple accounts; rather than using the single account. *Personal Experience to Misuse of Own Fake ID/ Multiple Accounts:* Among the offenders; who have already Fake ID; there are 98.46% people are directly involved in misuse of their accounts. *Preferable Medium/ Process of Misusing the Fake ID/ Account:* offenders generally make misuse their accounts via text, audio, image, video, extracting personal information etc. In here, most of the case offenders are fond of the event of anyhow extracting victim's personal information, about 34.4%, especially for female. Another 32.8% are involved in image relevant strategies and more 21.9%; people are involved misuse their account via Texting. Via video only 10.9% offender involved. *Preferable offences via Misusing the Fake ID/ Account:* There is variety of offences have become conducted via these mediums.

Those whom access victims' personal information, most of them usually involves in Cyber Stalking, (Personal Harassment of Victims) about 72.73%; in real world. Among rest, involves 13.64% directly things to black mailing to victims. The rest 13.64% not only make unauthorized access on victims' personal information but also tries to destroying it. Here, these charts clearly inform us about the vulnerability of unsafe personal information in Social Networking media account. In reality the offenders always try to collect information from female member account to make victimization. Among those whom Misusing the Fake ID/ Accounts (Via Image/Video/Text/Audio), about 45.24% involves in Unauthorized Publishing on Others Account for intentional purpose. Other, 33.33 % involves in Threatening/ Slung Text Related posting &rests 21.43% have involved in Pornography Related Publishing of image / video or both material on own or others accounts. *Offenders' Aftermath Assessment/ Feelings towards Victims:* Offenders have several strategically aftermath Assessment/ Feelings towards Victims. Most of them don't pay any kind of sympathy towards victims at any time before or after the crime, they feel they are at don't care mode, about 51.56%. Another 35.94%; have no feelings towards victims; neither they become reckless and nor they feel any guiltiness inside own & pay sympathy towards victims. Only 12.5% offender's having a soft corner towards victims. Sometimes they commit crimes via instant influence but after that at normal situation they felt on own guiltiness through self-justification.

Table-03: Profile of Victim's suffering orientation through Social Networking Site

Victimization have become conduct via	Social Networking Friend (50.0%)	Social Networking Group/ Community (9.76%)	Unknown Expert User (40.24%)	
Victimization Medium/ Method	Profile Information (96.34%)	Texting or sexting (2.44%)	Image (1.22%)	
Reason behind the Victimization Events	Poor Knowledge About Cyber World (42.68%)	Expert Hacking (28.56%)	Unawareness (Misuse of Trust) (15.85%)	Easy Password (13.41%)
Sufferings of Victimization	Incensement of Anxiety & Aggression (48.8%)	Metal Suspension (46.15%)	Social Insecurities (5.77%)	
Impact ness on Academic Aspect	Yes (75.61%)	No (24.39%)		
Academic Sufferings orientations	Loosing Concentration On Academic Study (90.32%)	Negative Treat From Fellows (08.06%)	Negligence (1.61%)	
Formal Complain to University Authority	Yes (0%)	No (100%)		
Reasons for not Issuing Formal Complain to University Authority, for remedy	Trying to Solve the Problem via outsource Capacity (47.56%)	Make Personal Negotiation With Offender (28.05%)	Lack of Reliability upon Authority (24.39%)	
The Responsibility/ Liability of the Victimization	Only Offenders (73.55%)	Both- the Perpetrator& the Victims (23.14%)	Only victim's (3.31%)	

Victimization Perspectives: The events of victimization have become conduct via three types of people or phenomenon's; the social Networking friends; the unknown user & the social Networking group/ community. Most of the victimization events have done by Social Networking Friend, about 50.0%, more about 40.24% victims have victimized via Unknown User. Only 9.76% have victimized via Social Networking Group/ Community (For most of case) after become a member of the community. *Victimization Medium/ Method:* As the medium of victimization, the victims have been victimized via different communicating elements of Social Networking Media. Most of the cases the events of victimizations have conducted through victims unsafe profile information (46.34%). More, 32.93% victimization occurs via texting or sexting (vaguer/ugly text or trying to blackmail towards female). Additionally, victimized through Image happened for 20.73% of cases. Top Reason behind the Victimization Events**:** Among the victims, 42.68% people think they become mainly victimized because of poor

knowledge about cyber world. 28.05% student faces vulnerability because of expert hacking. Only 15.85% students think they have been victimized mainly for unawareness about enough security of their virtual properties. The rest of 13.41% think that the unexpected event took place because of easy password of their account on social networking media.

Sufferings of Victimization: The sufferings orientation of victims never was a unique strategy. As some people already almost forget that event but most victims have to face some kinds of sufferings as the impact of the events. Among those whom have to suffer, about 48.08% students it cases incensement of anxiety & aggression; another for about 46.15% it cases metal suspension. More, 5.77% cases some level of social insecurities. *Impact on Academic Aspect:* For the victims, about 75.61% cases it cases immediate negative impact upon the academic prospects of the respondents. *Academic Sufferings Orientations:* Among the students whom feces negative academic impact; about 90.32% cases victims have lost their concentration on their academic study as the impact of this matter for several duration of time. Next 8.06% of student had to face negative treat from the fellows & others. Other 1.61% student experienced negligence from society. *Issuing Formal Complain to University Authority, for remedy:* It is surprise-able information that, along despite of these victimization events none of the victims have ever make any formal complain to university respective authority. *Reasons for not Issuing Formal Complain to University Authority, for remedy:* Throughout the study I have got several vital reasons; that's why victims are ever make any formal Complain to University Authority, for remedy. Among the victims, about 47.56% were tried to solve the problem via outsource means/ utilize their external links. About 28.05% students Mention about they have tried to solve the Problem privately via making personal negotiation with the offender. The rest 24.39% students think the problem can be solved via the university authority, if not able to produce effective result to solve and make peace about this problem, it may damage the students' creativity. *The Responsibility/ Liability of the Victimization:* Among the all of the respondents of the study there are 73.55% respondents think that the responsibility/ liability of the victimization mostly depends on the Offenders. Another proportion of students; about 23.14%, think this liability impose upon to the both- the offender & the victims of the crime. The only 3.31% respondents people think that the main reason of become victimized is the victim's incapacity to ensure the proper security on his/ her cyber space.

Bivariate Analysis

Cross-Table-01: Experience of Sufferings from Any Social Networking Hosting Site & Sex of the Respondent

Experience of Sufferings from Any Social Networking Hosting Site	Sex of the Respondent		Total
	Male	Female	
Yes	18.18%	49.59%	67.77%
No	32.23%	0%	32.23%
Total	50.41%	49.59%	100.0%

From the cross table-01, about "Experience of Sufferings from Any Social Networking Hosting Site" and "Sex of the Respondent"; we observed that from the total respondents about 67.77% students have already been victimized on using social networking media. Among this proportion the proportion of victimization of women is notably highest in count; about 49.59%. So more, especially we say that; the situation of victimization on Social Networking Hosting Site is moderately high; but in case of female victimization the situation is more vulnerable for young girls & women.

Cross-Table-02: Age Group of the Respondent &the Most Vulnerable Host-Site (From Bitter Experience of Victims)

Age Group of the Respondent	**The Most Vulnerable Host-Site (From Bitter Experience of Victims)**			**Total**
	Facebook	**YouTube**	**Twitter**	
16 -18 Years	04.88%	0%	0%	04.88%
19 - 21 Years	42.68%	0%	0%	42.68%
22 - 24 Years	41.46%	02.44%	01.22%	45.12%
25 - 27 Years	07.32%	0%	0%	07.32%
Total	96.34%	02.44%	01.22%	100.0%

On observing this cross-table-02, between Age Group of the Respondent and The Most Vulnerable Host-Site (From Bitter Experience of Victims); we find that the age group 22 -24 Years are most venerable on social networking media, about 45.12% victims are belonging at this age. The following age group 19 -21 years also are at most cautioning stage, about 42.68% victims are belonging at this age level. The offences have less impact upon the age level of 16-18 years, as this because the peoples of this level are less introduced and involved on social networking media than the other age levels peoples among the respondents.

Cross Table-03: Sex of the Respondent and Fake ID in Social Networking Media (S.N.M.), Measures of Lambda (λ)

Sex of the Respondent	Fake ID in Social Networking Media (S.N.M.)		Total
	Yes	No	
Male	61 (50.41%)	0	61 (50.41%)
Female	04 (3.31%)	56 (46.28%)	60 (49.59%)
Total	65 (53.72%)	56 (46.28%)	121 (100%)
Calculating Lambda **(λ)**		Value	0.931

From the Lambda (λ) Relationship cross table -03, here we observed that the symmetric neat value of the equation is 0.931. So we can say that there's very strong relationship between the Sex of the Respondent and Fake ID in Social Networking Media (S.N.M).

Cross Table-04: Suffering's Impact on Academic Aspect and The Most Vulnerable Host-Site (From Bitter Experience of Victims), Measures of Lambda (λ)

Suffering's Impact on Academic Aspect	The Most Vulnerable Host-Site (From Bitter Experience of Victims)				Total
	Facebook	YouTube	Twitter	Missing (N/A)	
Yes	61 (50.41%)	0	1 (0.83%)	0	62 (51.24%)
No	18 (14.88%)	2	0	0	20 (16.53%)
Missing (N/A)	0	0	0	39 (32.23%)	39 (32.23%)
Total	79 (65.29%)	02 (1.65%)	01 (0.83%)	39 (32.23%)	121 (100%)
Calculating Lambda **(λ)**		Value		0.792	

The Lambda (λ) Relationship cross table-04, explores the victimization feature on social Networking Media. Here, Symmetric value of the relationship between Suffering's Impact on Academic Aspect and The Most Vulnerable Host-Site (From Bitter Experience of Victims) is **0.792.** So the truth is there's an impact on academic orientation upon the victims, whom have become victimized on Social Networking Media in cyber Space.

Cross Table-05: Age Group of the Respondent vs. Number of Multiple Accounts of the Respondent, Measuring Correlation

Age Group of the Respondent	Number of Multiple Accounts of the Respondent					Total
	Two	Three	Four	Five	Missing (N/A)	
16 -18 Years	0	0	0	0	4	4
19 - 21 Years	5	2	0	0	31	38
22 - 24 Years	10	22	6	5	21	64
25 - 27 Years	8	3	4	0	0	15
Total	23	27	10	5	56	121
Calculating Pearson's Correlation (r)			Value		-0.518	

The cross table-06, Age Group of the Respondent vs. Number of Multiple Accounts of the Respondent shows that the value of Pearson's R is - 0.518. On interpreting this value here we can state that there is fundamental relationship available between these two variables & from this Coefficient Value we can easily predict that – after certain period of time (age level) as more as the age level increase, the number of the multiple account trends to decrease. Here from the chart we observed that the highest level frequency of the multiple accounts available on the age level 22 – 24 years. After that as the age level increase then the number of the multiple account decrease.

Cross Table-06: Daily Spending Time (Hour) on Social Networking Media (S.N.M.) - In Case of Regular User vs. Number of Multiple Accounts of the Respondent, Measuring Correlation

Daily Spending Time (Hour) on Social Networking Media (S.N.M.) - In Case of Regular User	**Number of Multiple Accounts of the Respondent**					**Total**
	Two	**Three**	**Four**	**Five**	**Missing (N/A)**	
1 hour	3	5	0	0	22	30
2 hour	15	8	3	1	22	49
3 hour	1	9	7	3	7	27
4 hour	1	3	0	1	0	5
5 hour	1	1	0	0	0	2
Missing (N/A)	2	1	0	0	5	8
Total	23	27	10	5	56	121
Calculating Pearson's Correlation (r)			Value		-0.154	

The cross table-07, have measure the relationship between Daily Spending Time [Hour] on Social Networking Media (S.N.M.) - In Case of Regular User vs. Number of Multiple Accounts of the Respondent. Here, we have get the Pearson's Correlation coefficient value as – 0.159. This indicates that the daily spending on social networking media actually not depends upon how many multiple account the user have. The truth is one user may have variety of multiple accounts but passes many hour in a specific account or some specific account (not in all the account in a day) for the fulfillment his/her desires and expectations. And for committing the cybercrime it is enough to use few specific accounts for specific strategies. Moreover, if we think as normal sense that using all accounts with its full capacities in everyday is nothing but a almost impossible & dream based unreal thinking.

Recommendations for Preventing Cybercrimes on Social Networking Media

Social networking sites have become a popular method of maintaining online contact with family, making new friends and networking. Unfortunately, unscrupulous individuals use social networking sites for identity theft, phishing, cyber-bullying and soliciting minors Just like any other technology terror, victimization of members in social networking

websites is on the rise and lack of adequate security mechanism in the deployment of these platforms compromises the security of its innocent users. Here some strategically recommendation for preventing social networking abuse and ensuring safety of all users. *Set Up of Boundaries:* It is important to think carefully about how public, users want his/ her profile or blog to be. The more identifiable the information user share, the more selective one should be with whom user share it. *Evaluate the Social Networking Site Before Use it:* Before becoming the member of any social networking, the uses must evaluate & explore the satisfactory answer of these Questions- Does it offers the level of control, protection, and overall experience that's right for user? Who's using it and how? Will users feel comfortable in this community? Carefully read the terms of use. Does the site claim ownership of user's information? Resell it? Use it to target ads to user? Moreover, Find out if and how vigorously the site monitors abusive interactions or inappropriate content and how to report these.

Beware of TMI: the five things should never be shared: Social networking means opening up and sharing information online with others, but there's some information that user should never share online. Protecting own self from sharing Too Much Information (TMI) can save user from identity theft and even protect users physical safety. So let's start with the obvious. Never share the social security number (including even just the last 4 digits), user birth date, home address or home phone number (although sharing of user's business phone is ok). Of course, users should protect all of own passwords, PIN numbers, bank account and credit card information**.** *Customize Privacy Options:* Social networking sites increasingly give users more control over their own privacy settings. Don't assume users have to take whatever default settings the site gives you. Checkout the settings, configuration and privacy sections to see what options have to limit who and what groups can see various aspects of user's personal information. Facebook probably has some of the broadest privacy options, giving the user control where no one, friends, friends and networks, or everyone can see basic info, personal info, photos, friends and postings. Search is a new area where users are gaining control of what others are allowed to see. Some sites let the users set the limits on who can see search results about you on the social networking site. *Don't Trust, Just Verify:* There are lots of reasons (most of them bad) why someone might impersonate or falsify an identity online. It could be as a prank or for "fun" such as those who impersonate a celebrity as satire. Faking an identity has a legit side too – it can be used by people who simply want to conceal who they are in order to protect their real. Before sharing too much information or

clicking on links; start by being on the lookout for anything unusual or out of the ordinary. If the content on the site doesn't look like or sound like the person the user knows, avoid it. E-mail or call other friend to verify the site is legit. Let them know, too, if one thinks someone else is faking one's friend's identity online.

Avoid accidentally sharing personal details: Users may never put a note on your front door stating, "Away for the weakened returning on Monday." Micro-blogging tools like Twitter and *What are you doing right now?* Features in Facebook, LinkedIn and other social networking sites make it easy to let details slip you wouldn't otherwise tell friends or strangers. Be aware of what information users put out there which others might use for nefarious purposes. Just keep that in mind as share tidbits of own life on micro-blogging tools. Users might want to be a little bit less specific in his/her tweets. *Search owns self:* It is a good idea to search own name on Google and check out own profile as others see it on social networking sites. Understand where own self show up and what information is available about own, and then adjust own profile, settings and habits appropriately. *Obviously Learn How Sites Can Use User Information:* Social network sites are typically free to use which means they are making their money by advertising to user. And that means they are collecting information about users. Is that information shared with outside companies and partners? What information can third-party plug-in software, such as Facebook Applications, use from user profile or page content? Review the site's privacy policy and watch closely the privacy settings you can control. Watch for this when anyone hear about an acquisition and always read notifications about changes to privacy terms, acceptable use policies and user agreements.

Use caution when users click links- that users receive in messages from other friends on social website. Treat links in messages on these sites as anyone would links in email messages. *Know the posted materials about yourself:* A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. To break into users account, they search for the answers to users' security questions, such as anyone's birthday, home town, high school class, or mother's middle name. If the site allows, make up own password questions, and don't draw them from material anyone could find with a quick search. For more information, see:

- What was the name of your first pet?
- What is screen scraping?
- Take charge of your online reputation

Don't make trust that a message is really from who it says it's from: Hackers can break into accounts and send messages that look like

they're from the users friends, but aren't. If users' suspected that a message is fraudulent, than use an alternate method to contact own friend to find out. This includes invitations to join new social networks. For more information, see Scammers exploit Facebook friendships. *To avoid giving away email addresses of own friends, do not allow social networking services to scan own email address book:* When any user join a new social network, he/she might receive an offer to enter own email address and password to find out if owns contacts are on the network. The site might use this information to send email messages to everyone in users contact list or even everyone ever sent an email message to with that email address. Social networking sites should explain that they're going to do this, but some do not. *Type the address of own social networking site directly into browser or use personal bookmarks:* If users click a link to the site through email or another website, users might be entering owns account name and password into a fake site where users' personal information could be stolen. For more tips about how to avoid phishing scams, see Email and web scams: How to help protect own self. *Be selective about who accept as a friend on a social network:* Identity thieves might create fake profiles in order to get information from users.

Choose the perfect social network carefully: Evaluate the site that plan to use and make sure about understanding the privacy policy. Find out if the site monitors content that people post. Must providing personal information to this website, so use the same criteria that user would to select a site where he/she enter his/her credit card. *Assume that everything users put on a social networking site is permanent:* Even if users can delete own accounts, anyone on the Internet can easily print photos or text or save images and videos to a computer. *Be careful about installing extras on the site:* Many social networking sites allow users to download third-party applications that let users do more with own personal page. Criminals sometimes use these applications to steal users' personal information. To download and use third-party applications safely, take the same safety precautions that one 'stake with any other program or file users download from the web. *Think twice before using social networking sites at work:* For more information, see be careful with social networking sites, especially at work. *Talk to friends/ kids about social networking:* If anyone having a parent of friends/ children who use social networking sites, see How to help own friends/ kids use social websites more safely.

Conclusion

The 21st Century has already been called as the century of Information& Technology- this information& technology is for life security, safety and

enhancements. Today's life becomes busier on day by day. The utilization perspectives of Social Networking Media are to facilitate this busy life via connecting lives on the busy world. The informative technology & creative ideas have mix-up in the line of the enhancement of social networking media. Whatever, people may remain wherever any corner of the world he/ she my get connected or in touch always with the friends, relatives & other desirable persons via different Host site of Social Networking Media. This technological enhancement remain available as much as anyone desires to fulfill all his/her communicating requirements with very... very cheap rate all over the globe; so the popularity of social networking media have been increasing day after day. There has proved that where is light; there must be the presence of darkness; in other words, the good & evil walks along side by side. In respect of social networking media, these days it has also become the true event. As one side the social networking media paves the new dimension in communication and sharing information purpose inconsistent with the busy life; on the other side it also opens the facility of originating new forms of criminal activity in the cyberspace. These creates dilemma and hazards on modern life. Sometimes it goes on severe level on its impact these types of adventurous crime attract the educated youth- adults most by its nature & orientation of attributes. This crime is basically happens because the user either have not the sufficient knowledge about up-to-date facilities& security strategies of his/her account on social networking media or expertness of the cyber offender due to some systematic loopholes of the service providing Social Networking Site. Whatever the matter, these orientations of cybercrimes really increase the vulnerability of civilized life on both virtual and real perspectives. The strategies of Social Networking Media are one of the modern civilized life effective phenomenons. It connects, ultimately converts the far & busy life into close (near) & easy Life/ orientations. We must not make it unsafe & vulnerable to its users for the sake of global peace and inter-faith harmony in both virtual and real life context, we need to act NOW, before it is too late to make done all that needs protect via make safe & reliable means of sharing the moments of life with others rather than make abuse it. We only have one world cyber space, and we cannot afford to let it go inside the tight grips of the cyber criminals.

Glossary:

AOL: AOL Inc. (previously known as America Online) is an American global Internet services and media company. AOL is best known for its online software suite, also called AOL that allowed customers to access the world's largest "walled garden" online community and eventually

reach out to the Internet as a whole. At its prime, AOL's membership was over 30 million members worldwide. (en.wikipedia.org/wiki/AOL, 2011)

BBS: An electronic message center. Most bulletin boards serve specific interest groups. They allow you to dial in with a modem; review messages left by others, and leave your own message if you want. Bulletin boards are a particularly good place to find free or inexpensive software products. In the United States alone, there are tens of thousands of BBS. (en.wikipedia.org/wiki/Bulletin_board_system, 2011)

CFO: The executive who is responsible for financial planning and record-keeping for a company. (www.investorwords.com/852/Chief_ Financial_Officer.html#ixzz1ZoPBJihU, 2011)

CompuServe: CompuServe Information Service: Short for CompuServe Information Service, one of the first and largest online services. CompuServe supports a wide array of forums and provides many types of electronic-mail services. In addition, it is connected to hundreds of different database systems. In 1997, the content portion of CompuServe was acquired by America Online and the network service was acquired by WorldCom. (en.wikipedia.org/wiki/CompuServe, 2011)

Internet Crime Complaint Center: The IC3 was established as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. The IC3 was intended, and continues to emphasize, serving the broader law enforcement community to include federal, as well as state, local, and international agencies, which are combating Internet crime and, in many cases, participating in Cyber Crime Task Forces. (www.ic3.gov/ about/default.aspx, 2011)

Jaiku: Jaiku is a social networking; micro-blogging and life streaming service comparable to Twitter. Jaiku was founded in February 2006 by Jyri Engeström and Petteri Koponen from Finland and launched in July of that year. It was purchased by Google on October 9, 2007. While it does have the 140-character limit that most micro blogging tools have, it offers other features that make it attractive to users. Jaiku offers threaded messaging and threaded comments functionality (other micro blogging tools offer no threading or threading of messages only). Additionally, users can create smaller "channels" to separate conversations, and mobile and third-party applications are available. (http://social-networking.findthebest.com/q/87/357/What-is-Jaiku-social-networking-site, 2011)

LinkedIn: LinkedIn is a business-related social networking site. Founded in December 2002 and launched in May 2003. LinkedIn is the world's largest professional network with over 120 million members and growing rapidly. LinkedIn connects you to your trusted contacts and helps you exchange knowledge, ideas, and opportunities with a broader network of professionals. (en.wikipedia.org/wiki/LinkedIn, 2011)

Orkut: Orkut is a social networking website that is owned and operated by Google Inc. The service is designed to help users meet new and old friends and maintain existing relationships. The website is named after its creator, Google employee Orkut Büyükkökten. Although Orkut is less popular in the United States than competitors Facebook and MySpace, it is one of the most visited websites in Indian Subcontinent and Brazil. (http://en. wikipedia.org/wiki/Orkut, 2012)

Social Capital Theory: Boyd and Ellison (2007) noted that "the bulk of SNS research has focused on impression management and friendship performance, networks and network structure, bridging online and offline connections, and privacy issues" (p. 219). Of concern here is the potential of SNS to bridge or create a gap between online and offline connections a key component of social capital theory.

Web 2.0 opportunity: Internet applications that facilitate interactive information sharing, interoperability, user centered design and collaboration. Applications such as Facebook (online social network), Flickr (online image-sharing community) and YouTube (online video sharing community) are already used by cultural organizations that interact in the informal context of Web 2.0 (http://www.ariadne.ac.uk/issue63 /nogueira/, 2011).

Reference

Adamic, L. A., Büyükkökten, O., & Adar, E; (2003); A social network caught in the Web. First Monday,8 (6). Retrieved 11 November, 2011, http://www.firstmonday.org/issues/issue8_6/adamic/index.html

Akers, Ronald L. (1994); Criminological Theories: Introduction and Evaluation, Roxbury Publishing Company, California, USA.

Anderson, D. A. (1999), Baker Thersher L.: Doing Social Research; California State University, San Marcos, Third edition.Wadsworth/Thomson Learning, Inc., and Belmont, CA, USA.

Blalock Hurbert M. (1960); Social Statistics; McGraw-Hill Series in Sociology.

Boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11.

Criminology and Criminal Justice Department at Portland State University (2011); Retrieved November 11, 2011, http://online.ccj.pdx.edu/facebook-may-be-the-future-of-cyber-crime-800552845.

Christopher Nickson (2009); *The History of Social Networking*; Retrieved October 5, 2011, http://www.digitaltrends.com/features/the-history-of-social-networking

David Barrett, PA Home Affairs Correspondent (2007); *Crime risk warning to users of social networking sites;* Retrieved October 5, 2011, http://www.independent.co.uk/news/uk/crime/crime-risk-warning-to-users-of-social-networking-sites-400062.html

EgovAsia Editors (2010); *Online crime continue to rise in social networks*; Retrieved November 11, 2011, http://www.enterpriseinnovation.net/content/online-crime-continue-rise-social-networks.

Garry Barker (2010); *Cybercrime in your Facebook*; Retrieved November 11, 2011, http://www.smh.com.au/digital-life/digital-life-news/cybercrime-in-your-facebook-20100715-10bvo.html

Hansen, William B. and Reese, Eric L; (200. Network Genie User Manua.; Greensboro; NC: Tanglewood Research

Jim Finkle (2009); *Cybercrime spreads on Facebook*; Retrieved November 11, 2011, http://www.reuters.com/article/2009/06/29/us-facebook-security-analysis-idUSTRE55S55820090629

Kevin Voigt (2009); *Twitter message could be cyber-criminal at work*; Retrieved November 11, 2011, http://articles.cnn.com/2009-06-21/tech/cyber.crime.internet_1_cyber-criminals-cyber-crime-mcafee?_s=PM:TECH (A. Date: 11 November, 2011)

Matthew L James (2010); *Cyber Crime 2.0 versus the Twittering classes*; Department of Parliamentary Services; Parliament of Australia, Australia; Rtrieved November 11, 2011, www.aph.gov.au/library/pubs/bn/sci/Cybercrime.htm

Mary Landesman (2009); *Facebook: A new battleground for cyber-crime* ; Retrieved November 11, 2011,h http://www.euractiv.com/infosociety/facebook-new-battleground-cyber-crime/article-184380 (A. Date: 11 November, 2011)

Maxfield Michael G. and Babbie Earl (1995); Research Methods for Criminal Justice and Criminology; Wadsworth Publishing Company, USA.

Melissa (August 11, 2011); *Dangers of Social Networking Sites; Businesses, Job Seekers, Children and Adults Beware*;Retrieved November 11, 2011, http://www.optimum7.com/internet-marketing/social-media/dangers-of-social-networking sites.html

Michele L. Ybarra & Kimberly J. Mitchell PhD (2008); *How Risky Are Social Networking Site, A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs*; Retrieved November 11, 2011, http://pediatrics.aappublications.org/content/121/2/e350.full

Michelle Kessler (2009); *Facebook users under cyberattack* ; Retrieved November 11, 2011, http://content.usatoday.com/communities/technologylive/post/2009/10/620000630/1

Mitchell Ashley (2008); *12 tips for safe social networking*; Retrieved November 11, 2011, http://www.networkworld.com/community

Nachmians Chava Frankfort and Nachmians David (1996); Research Methods in the Social Science; J W Arrowsmith Ltd., Bristrol, Great Britain.

Neeraj Chauhan (February 12, 2011); *Social networking sites hunting ground for cyber criminals*; The Times of India; Retrieved November 11, 2011, http://articles.timesofindia.indiatimes.com/2011-02-12/delhi/28542889_1_social-networking-sites-profiles-complaints

Priyankan Goswami (2011); *Exploitations in Facebook and cybercrime – Growth of a social curse* ; Retrieved November 11, 2011, http://www.timesofassam.com/ headlines/exploitations-in-facebook-and-cybercrime-%E2%80%93-growth-of-a-social-curse/

Rajeev Saxena (2009); *Facebook Now Marred By Cybercrime*; Retrieved November 11, 2011, http://trendsupdates.com/facebook-now-marred-by-cybercrime/ (A. Date: 11 November, 2011)

Samanth Murphy (2011); *Facebook Crimes on the Rise, Experts Warn*; Technology – Scitech; Retrieved November 11, 2011, http://www.foxnews.com/scitech/ 2011/08/11/facebook-crimes-on-rise-experts-warn/

Stephanie Chen (2009); *Facebook, Twitter users beware: Crooks area mouse click away, CNN*; Retrieved November 11, 2011, http://articles.cnn.com/2009-10-19/justice/social.networking.crimes_1_social-networking-sites-director-of-threat-research-facebook?_s=PM:CRIME

Tanuj Lakhina (2011); *Crime on Social Networks–reason to put you off?*; Retrieved November 11, 2011, http://www.indiasocial.in/crime-on-social-networks-%E 2%80%93-reason-to-put-you-off/

THE HINDU REPORT (2011); *Facebook crimes on the rise- say experts*; Retrieved November11,2011,http://www.thehindu.com/scitech/internet/article2356912.ece

Therese L. Baker (1999); A Theoretical Framework. In Doing Social Research, International Edition, McGraw-Hill Companies, USA. p. 251-252.

Vold, George B.; Bernard, Thomas J.; and Snipes, Jeffrey B. (1998). Theoretical Criminology, Fourth Edition, Oxford University Press.

11 tips for social networking safety (2010); Microsoft® Safety & Security Center; Retrieved November 27, 2011, http://www.microsoft.com/security/online-privacy/social-networking.aspx

Internet web-page:

http://www.ariadne.ac.uk/issue63/nogueira/ (A. Date: 15 November, 2011)

http://www.aph.gov.au/library (A. Date: 15 November, 2011)

http://en.wikipedia.org/wiki/Bulletin_board_system (Accessed September 28,2011)

http://en.wikipedia.org/wiki/CompuServe (A. Date: 11 November, 2011)

http://en.wikipedia.org/wiki/AOL(A. Date: 15 November, 2011)

http://en.wikipedia.org/wiki/Facebook (Accessed on 25 October, 2011)

http://en.wikipedia.org/wiki/Friendster (A. Date: 15 November, 2011)

http://en.wikipedia.org/wiki/LinkedIn(A. Date: 15 November, 2011)

http://en.wikipedia.org/wiki/Myspace (Accessed on 25 october, 2011)

http://en.wikipedia.org/wiki/Twitter (A. Date: 15 November, 2011)

http://www.fidonet.org/inet92_Randy_Bush.txt (Accessed September 28, 2011)

http://www.fidonet.org/inet92_Randy_Bush.txt (A. Date: 15 November, 2011)

http://www.foxnews.com/scitech/2011/08/11/facebook-crimes-on-rise-experts-warn/ (A. Date: 15 November, 2011)

http://www.hubspot.com/.(A. Date: 11 November, 2011)

http://www.ic3.gov/about/default.aspx (Accessed on 25 October, 2011)

http://www.independent.co.uk/news/uk/crime/crime-risk-warning-to-users-of-social-networking-sites-400062.html (A. Date: 11 November, 2011).

http://www.internetsafety101.org/Socialnetworkingstats.htm (A. Date: 26 November,2011).

http://www.investorwords.com/852/Chief_Financial_Officer.html#ixzz1ZoPBJihU (Accessed September 28, 2011)

http://www.reuters.com/article/2009/06/29/us-facebook-security-analysis-idUSTRE55S55820090629 (A. Date: 25 October, 2011)

http://en.wikipedia.org/wiki/Orkut, A. Date: 2 August, 2012)

http://social-networking.findthebest.com/q/87/357/What-is-Jaiku-social-networking-site(A. Date: 11 November, 2011)

http://www.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/sophos-security-threat-report-jul-2009-na-wpus.aspx (A. Date: 11 November, 2011).

http://www.timesofassam.com/headlines/exploitations-in-facebook-and-cybercrime-%E2%80%93-growth-of-a-social-curse/(A. Date: 25 October, 2011)

http://tweeternet.com/(A. Date: 11 November, 2011)

http://what-is-what.com/what_is/youtube.html (Accessed on 25 October, 2011)

http://www.whatissocialnetworking.com/(Accessed on 03 december,2011).