International Journal for Empirical Education and Research

Prevention of Cyber Crime in Bangladesh

Ahasn Sheikh

Department of Law

American International University-Bangladesh

Email: ahsanllb0@gmail.com (Author of Correspondence)

Bangladesh

Abstract

Cybercrime covers such a broad scope of criminal activity; the examples above are only a few of the thousands of crimes that are considered cybercrimes. While computers and the Internet have made our lives easier in many ways, it is unfortunate that people also use these technologies to take advantage of others. Therefore, it is smart to protect yourself by using antivirus and spyware blocking software and being careful where you enter your personal information. So from above discussion we can say that, Cyber means committing any crime by using computer or any act which is forbidden by law, by using information technology.

Keyword: Cyber Crime; Origin and Development; Cyber law; Awareness; Reason; Prevention.

ISSN Online: 2616-4833 ISSN Print: 2616-4817

1. Introduction

Advancement of technology not only widens scientific horizon but also poses constant challenges for the jurisprudence, legal system and legal world as a whole. Computers, internet and cyberspace together known as an information technology presents challenges for the law. Challenges, which are not confined to any single traditional legal category but in almost all established categories of law such as criminal law, contract, tort, as well as legal concepts of property, expression, identity, movement etc. Existing legal system and framework has shown the inadequacy of law while dealing with information technology itself as well as while dealing with the changes induced by the information technology in the way of our living. The courts throughout the world have been dealing with those problems. Presently, the law providing answers to these problems or dealing with the information technology is termed as 'computer laws' or 'Information technology laws' or 'cyber laws'

2. Meaning of Cyber-Crime

Cyber means "computer" or "computer network," commonly used as cyberspace, cyber Culture, cyberpunk, the electronic medium in which online communication takes place. Anything related to computer is also termed as cyber. Now more than hundred words are constructed using the prefix of cyber. Commonly used word for these crimes is "Cybercrime". Mostly it is used to denote Insecurity in cyberspace although in itself it appears to be a meaningless word. Usually it also signifies the occurrence of harmful behavior done through the misuse of computers or through networked computers. Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. Two of the most common ways this is done is through phishing and harming. Both of these methods lure users to fake websites (that appear to be legitimate), where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity. For this reason, it is smart to always check the URL or Web address of a site to make sure it is legitimate before entering your personal information. Cybercrime covers such a broad scope of criminal activity; the examples above are only a few of the thousands of crimes that are considered cybercrimes. While computers and the Internet have made our lives easier in many ways, it is unfortunate that people also use these technologies to take advantage of others. Therefore, it is smart to protect yourself by using antivirus and spyware blocking software and being careful where you enter your personal information.

So from above discussion we can say that, Cyber means committing any crime by using computer or any act which is forbidden by law, by using information technology.

3. Origin and Development of Cyber Crime

Origin of the cyber-crime was from the origin of the computer, which we can say from the era of mainframe computers. Professor Susan W. Brenner in his book Cyber Crime divided the origin of cybercrime in two phases, first from the era of mainframe computers to 1990, when the internet and personal computers were becoming more sophisticated and more pervasive. And the other phase is from 1990 to present. More easily we can divide the origin of cybercrime in two periods, one, before the internet and the other after emergence of Internet, because 1990 was the time when internet was spreading very fast around the globe.

4. Cyber Crime after Emergence of Internet

The other phase was distinguished since the commercialization of the Internet in the mid1990's; this was the period when internet growth was tremendously fast. This was the time when the Personal computers and Internet were becoming increasingly sophisticated. In December 1995 there was an estimated 16 million Internet users worldwide, by May 2002, this figure had risen to over 580 million, almost 10 percent of the world's total population. (NUA, 2003). But this was also the fact that this rise is unequal for the worlds, for example, over 95 percent of the worldwide total internet connections are located in the USA, Canada, Europe, Australia and Japan. And this was the time when the new type of crime was introduced in the history of crime which sensitized the utilities of the internet. In the initial phase of the computer technology and cybercrimes, the more often used word was "Hacking', at that time it was common to use the word hacking more frequently than cyber-crime, although later hacking was established as one of the crimes comes within the ambit of cybercrimes. The most notorious hacker was Kevin Mitnick back in 1990's, he was the member of the gang who usually indulge their selves in phone preaching but later at the advent of computer, Kevin made himself familiar to computer technology and got fame as a hacker. For his mischievous activities, he even faced the trail and got convicted when he was only 17. Later on violation of probation period, he was arrested and confined for 6months. After release he did few jobs and learned more about computers and hacking. In 1987 he was held for the unauthorized access to a computer and again put on probation. And his journey went to 2005, often arrested and confined. Kevin was like a fear for everyone even after his arrest. During this time many individuals and groups were arrested and discovered having same activities as Kevin did and other developed wrongful things. In 2006, for example, federal agents arrested two men who were accused of hacking to steal phone service and resell it for a profit. One of them Edwin Pena, created two companies to sell discounted telephone service. He hired Robert Moore to hack the networks of 15 communications

providers and “hundreds of businesses” and steal the phone service Pena sold. Prominent cybercrimes done in its history through various methods like in 2000, computers users received email with the subject line “I LOVE YOU” and with the attachment entitles LOVELETTER FOR YOU. Txt.vbs. On opening of this attachment the computer automatically send this virus to the addresses to the people in address book of the recipient and thus creating trouble for many individuals and corporations. And that was the time many countries found the problem while investigating this LOVE BUG virus and the problem was no availability of laws for these kinds of crimes. Even many states of USA do not have the laws. After passing every day cybercrime is taking different forms and shapes. Today, world is so dependent on the electronic devices that from school studies to big business transactions individuals and the corporations are using computer and electronic devices to manage their affairs. People can handle being at their homes, from their accounts to their companies under one click. This kind of technology development is leaving a large area for the protection of the individuals and the group of people. The security of the people is only possible through protected mediums and in case of any criminal act; laws should be so strict to punish any criminal to avoid any other similar happening. Next part of this work will examine the legislative development in the cybercrime area.

5. The Nature of Modern Cyber Crime

Today, criminals that indulge in cyber-crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day’s work.

Cyber-crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber-crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals. Mobile threats**,** particularly from mobile devices are clearly on the rise. As we are all now aware, PC sales are decreasing: according to recent reports, global sales for PC’s declined for the fifth consecutive quarter in the April-June period, which makes that the longest decline in the PC market’s history. With the increase of hand-held devices means that there is an increase on attacks directed at the devices. For example, targeting mobile banking transactions is possibly the biggest threat out there. BYOD also fits into this category. (Side note: if you are interested in cell phone pen testing and security check out our Hacker Hotshot with Georgia Weidman and for BYOD – Aamir Lakhani).

The Privatization of Financial Banking Trojans and Other Malware is EMC's second predicted large-scale threat of 2013. Activism and the Ever-Targeted Enterprises. We all know about Hacktivism, there's no need to explain that. (Side note: completely different subject but you might find this post interesting! Cast your poll for the best hactivist hacking group logo! Last check we had 73 votes.)

5.1. Cyber Crime against Individual

Email spoofing, spamming, cyber defamation, harassment and cyber stalking are examples of cyber-crime against individual. Email spoofing is a spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source . Then, the crime of spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters. While cyber defamation occurs when defamation takes place with the help of computer or the internet. For example when someone publishes defamatory matter about someone on a website or send e-mails containing defamatory information. While cyber stalking means following the moves of an individual's activity over internet. It can be done with the help of many protocols available such as e-mail, chat rooms or user net groups.

5.2. Cyber-crime against property

The common cyber-crime under this category is credit card fraud. Tommy Sea in an article published in thenewnewinternet.com mentioned that "the most widespread of financial crimes in Malaysia were financial statement frauds, procurement frauds and misappropriation of assets". According to Malaysian national news outlet Bernama, financial and cyber-crimes are the most common crimes committed in Malaysia.

Credit cards are meant to make life easier, it is a substitution to real cash, therefore some people refer it as the 'plastic' money for we need not to worry of losing our money or misplaced our full of cash wallet anywhere. Even though if we ever lost our credit card in the street, our money will still be safe because it is protected by our signature and PIN numbers and password. However when credit cards are being used widely on the Internet for online shopping or online banking, it become dangerous. Just at the click of the mouse; our saving could be wiped out in a split of seconds due to our own negligence. According to ChoongWai Hong (the chief of Maybank Virtual Banking), there were 1,200 online banking fraud traced between January and June in 2008 alone which involved RM348.5 billion transaction and RM 1 million lost. Other than fraud, there is another method of crime against property in the Internet which is known as Salami Attack. It is a series of minor attack onto unsuspecting victims that together will results in a larger attack. For example, an offender steals 10 cent from everyone's account around the world through online banking. Just imagine the sum of money he will able to acquire if he succeeded. Another type of cyber-crime against property is intellectual property crimes which includes software piracy, illegal copying of programs, distribution of copies of software, songs, movies,

and so on. It involves copyright infringement, registered trademarks violations and theft of computer source code. In other word, it is known as piracy which involve illegal reproduction and distribution which causing monetary loss to the original owner. Example of web site that had been closed down due to copyright issue was napster.com.

Another cyber-crime under this category will be the 'Internet Time Theft'. It is a situation where the usage of the Internet hours were used by an unauthorized person but actually paid by another person. This is done by gaining access to the login ID and password of the unsuspecting payer as in Colonel Bajwa's case in India.

5.3. Cyber Crime against Organization

An unauthorized accessing of computer which is accessing the computer or network without permission from the owner is one of the instances of this type of cyber-crime. It can be of two forms. The first one is changing or deleting data. While the second form is computer voyeur. It is when the criminal reads or copies confidential or proprietary information but the date is neither deleted nor changed. The other example of crime against organization is denial of service. When internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server. Virus attack is also one of the examples of crime against organization. A computer virus is a computer program that can infect other computer programs by modifying them in such way as to include a copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms unlike viruses do not need the host to attach them to. Furthermore, the email bombing in order sending large numbers of mails to the individual or company or mail servers thereby ultimately are resulting into crashing also crime against organization.

5.4. Cyber Crime against Society

Cyber terrorism may also be categorized as a crime against society where it main target may be against women, children, race or even a group of people. As mentioned earlier the cyber-crime may be over lapped under each classification but against the different group target as a victim. Modus operandi or the criminal act will be still the same. The main purpose is to intimidate or to coerce others so as to follow and fulfill their objectives.

Usually offender will hacks into the website of another and gain access and control over, the offender then further change the content of the website based on their either political objective or for money. Some even go beyond with the intention to sabotage the website.

6. Comparison between Ordinary Crime & Cyber Crime

Crime is the breaking of rules or laws for which some governing authorities can ultimately prescribe a conviction. The offender is visible and punished approximately. The trial and punishment procedure is

specified in the statute. On the other hand "offences that is committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modem telecommunication networks such as internet (chat rooms, emails, notice boards and groups) mobile phone. The offender is remaining out of reach, because the offence is done by using computer, internet and mobile phones. So now it can be understood that cyber-crime both are offences which is punishable by law. The difference cyber-crime done through computer or network, the offender is not apparently involved with the commission of crime where in case of ordinary crime, the offender is bodily involved or apparent in the commission of crime. But both the crime is done intentionally to harm the victim bodily or mentally.

7. Cyber Crime in Bangladesh

Development of Science and ICT depends on the expansion of telecommunication sector. This sector is still under developed due to lack of deregulation and open competition. The impact of cyber-crime is not alarming Bangladesh because financial transactions have not yet been fully facilitated in online. As soon as financial transactions are allowed online computer crimes will increase at an unprecedented rate unless the Government acquires the tools and infrastructure to prevent, detect and prosecute them but our government still not aware of the fact. Internet services provided through the local area network are vulnerable to similar attacks and intrusions by hackers more often when the security level is inadequate. Now a day in Bangladesh some people send malicious mail to different foreign diplomatic Mission and other VIPs which sometimes cause serious problem for the police and also for the government. Some people use internet for transmitting false and malicious data. Some of them use internet for women and child trafficking. Pornography is another dangerous business weapon of the cyber criminals. But In spite of this the Government of Bangladesh is not alert. Life is about a mix of good and evil. So is the Internet. For all the good it does us, Cyber space has its dark sides too. Unlike conventional communities though, there are no police men patrolling the information superhighway, leaving it open to everything from Trojan horses and viruses to cyber stalking, trademark counterfeiting and cyber terrorism. Few months earlier one group of people hack the web site of Rapid – action – battalion in Bangladesh. When this incident was published in the media all most all the institution of the government became scared. Nobody wants to believe it. After that RAB arrested some people and they are now in jail. One of the main RAB website hackers, ShaheeMirza, said that nobody should use his acquired computer skills in such criminal activities like hacking of important Government or private websites. After listening his statement lot of expert who are dealing with cyber-crimes in Bangladesh become scared. Although the 2006 Information and Communications Technology (ICT) Act covers many of the legal aspects to prosecute cyber-crime, but it has not been effectively implemented since its ratification. According to the expert opinion the main reason

for the law's Ineffectiveness, is the lack of legal support and social and public awareness about Computer crimes. Cyber-crime analysts point out that although pornography is not considered illegal across the world, but in Bangladesh it is one of the predominant computer crimes. There is already evidence of the existence of illegally hosted pornographic websites with local content. In Bangladesh, Nowadays youths are increasingly using cyber cafes as their dating places. According to newspaper reports, various types of antisocial activities take place in these cafes in the name of net browsing. For Internet browsing, there are separate cabins for pairs where their intimate moments are videoed secretly. These pictures are later made available on the Internet. According to section 57 of the ICT Act 2006, a person convicted for uploading vulgar and obscene contents on website is punishable to a 10-year imprisonment and a fine of Tk one core. But no one care it because in our country we still do not have any effective cyber tribunal to deal with this problem. That is why it is very easy for the cyber criminals in Bangladesh to get rid of punishment.

8. Cyber law in Bangladesh

Bangladesh is planning stringent measures to fight cyber-crime amid the rapid expansion of the information and communications technology and telecommunications networks in the South Asian country. Bangladesh's ICT industry has been expanding exponentially and is making its presence strongly felt both in the public and private sectors. More than five million personal computers are now in use in the country with three million internet users, by industry estimates. "We have taken steps to facilitate fair and secured use of information technology as the country lacks a complete law to deal with cyber-crime," says MM Neazuddin, Joint Secretary to the Science and ICT Ministry. Neazuddin said that the government, which has pledged a "Digital Bangladesh" by the year 2021, had approved in principle to amend previous legislation calling for jail terms and heavy financial penalties to tackle new forms of crime. The proposed law has suggested provisions for a maximum 10 years in jail and taka 10 million (US$150, 000) in fines for hacking into computer networks and putting false and libelous information or indecent material online. For the speedy and effective prosecution of the offences, the government will consult with the Supreme Court to set up one or more Cyber Tribunals.

8.1. The Information and Technology Act, 2006

The Penal code of Bangladesh contains very few provision regarding cyber-squatting. But in case of cyber-crime like Hacking, Internet time thefts, Email bombing- there is nothing contained in our penal code. So it can be said that it is not possible for our government to control cyber-crime by using some provision of the penal code. To controlled cyber-crime it is necessary to enact special law which only deals with cyber related matters. The Government of Bangladesh passed Information Technology Act on 2006. This is the most recent statute enacted by the government of Bangladesh with a view to consolidate Computer related matters and also

prosecute computer and computer network related Offence. This statute contains several provisions regarding damage to computer and computer system. Cybercrime dictates that prohibits attacks or unauthorized access to computers and computer systems. According to Section 66 of the ICT Act provides Punishment for tampering with computer source documents. Section 66 says whoever intentionally destroys or alters or intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs or with both. Section 67 Hacking with computer system. Whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any other person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of "hacking". Section 68 of the ICT Act provides punishments for the hackers. Section 68 says that whoever commits hacking shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to taka two lakhs or with both. But the problem of this act is this act deals with so many things. The act is made to cover all the information technology related matters. But it is not possible to cover all the things by implementing just only one act. In order to control cyber-crime we need to have one specific cyber law in our country.

8.2. Necessary to Establish a Cyber Tribunal in Bangladesh

Bangladesh has formed a fast-track court to try cyber criminals after a spike in crimes involving mobile phones and social networking sites such as Face book. The move comes four months after major communal violence in which an alleged Face book posting of a photo defaming the Koran by a Buddhist sent tens of thousands of Muslims on the rampage against the minority community. Officials said the Cyber Tribunal, the first of its kind in the country, will be empowered to conclude trials within six months. The report related to cyber-crime tribunal suggested that this tribunal was needed for the sake of quick and efficient trial of cyber-crime cases as they disturb social stability. BTRC are receiving a growing number of complaints about abuse and harassment using fake Face book IDs, doctoring photos, filming porno footage with mobile phone and posting them on websites and hacking of websites. The BTRC set up a taskforce to deal with the cyber-crimes last year and it was "overwhelmed with thousands of complaints", he said. Last year police arrested at least half a dozen people after they allegedly made derogatory comments and posted doctored photos of Prime Minister Sheikh Hasina on their Face book accounts.

9. Awareness of Cyber Crime

Educational institutions may include curriculum comprise with moral and social ethics and users' code of conduct for the future IT fellows not to use the technology in a morally reprehensible manner. Law enforcement authority must monitor cafes' and users' activities imposing restriction on some websites and users (under18) requiring bar code/password for use and make the users aware of the possible consequences of using certain sites. A "citizen" should always rethink whether his activities render him vulnerable and keep in mind the following things:

a) To prevent ID theft one should avoid disclosing personal information (DoB, bank details) on any web site to strangers.
b) Avoid sending any photograph online and providing email address to unknown person or chat friends as there may be misused of it.
c) Unexpected financial gain offered by any person without any consideration should be avoided unless the person is close relative, one may be asked to provide some intrinsic information (address, DoB, bank details), transaction/service charges.
d) Always uses latest and update antivirus software to guard against virus attacks and keep back up volumes so that one may not suffer data loss in case of virus attack.
e) Parents should keep an eye on children that are accessing internet to protect them any abusive or immoral illusion and imminent danger. Finally, it may be submitted that the collective effort of state and nations is only a possible way to see the peoples' dream of a Digital Bangladesh in existence and could protect individuals and national security of the state from the aggression of cyber criminals.

10. Reason for Cyber Crime

The Concept of Law has said that the 'Human Beings are Vulnerable so the rule of law is required to protect them'. Applying this to the Cyberspace, we may say that computers are vulnerable so the rule of law is required to protect and safeguard them against the Cyber Crime. The reasons for the vulnerability of computers may be said to be:

Academic institutions and intergovernmental organizations are important stakeholders in the prevention and combating of cyber-crime. Such institutions may contribute, in particular, through knowledge development and sharing; legislation and policy development; the development of technology and technical standards; the delivery of technical assistance; and cooperation with law enforcement authorities.

Knowledge development and sharing – In response to governmental and industry demands for cyber security professionals and workforce development needs, academic institutions have established specialized

educational programs, curricula and training centers consolidate knowledge and research, and increase synergies in knowledge across domains and disciplines. A growing number of universities offer degrees, certificates, and professional education in cyber security and cyber-crime related topics to promote 'educating and training young adults and future professionals about safe computing practices and technical matters'. Universities also promote applied learning and the development of social networks against cybercrime through the organization of workshops and conferences. These provide opportunities for the exchange of information and advice on preventative and response measures, the cultivation of informal cooperation, and, at times, mechanisms for specific act reporting and development of technical solutions. Academic contributors to cybercrime control efforts come from a wide range of disciplines, including computer science and engineering, law, criminology and sociology. The past two decades have seen a significant growth in the number of academic journals dedicated to issues related to cyberspace, cyber security, and cybercrime. Awareness and research on related issues has resulted in an increasing number of technical reports, research and peer-reviewed publications, agency data analysis, and unpublished proprietary research. University specialists provide a significant contribution to the development and amendment of legislation and policy. At the national, regional, and international level, academics provide legal advice and draft legislation on a range of topics, including criminalization, confidentiality and privacy, constitutional and legal protections. Such advice is delivered through a range of mechanisms, including participation in advisory groups and task forces, institutional and individual contracts, and through technical assistance programs. One academic respondent, for example, noted that dedicated cyber research centers frequently act as coordinators: 'of activities of specialized researchers within different work areas related to cybercrime (legal, criminological, technical expertise)'.Technology and technical standards –Universities undertake pure and applied scientific research on computer technology, either in the context of academic-private sector and/or government cooperation, internal or external sponsored research, or as a means to secure the university network. Universities may also contribute to computer forensics, evidentiary analyses and agency data analyses. In addition to institutional and individual research, universities also represent important partners and facilitators of cooperation, through participation in professional organizations and standards organizations, as well as technical working groups. A few national cyber security strategies explicitly mention the role of universities in efforts to secure cyberspace. In conjunction with knowledge development and technical assistance activities, a few universities have developed special educational programs, for example, in cybercrime investigations and digital forensics, to which police and governmental authorities formally second their employees as students. One respondent noted, for example, that: 'There are no general institutionalized grounds for cooperation - state agencies have neither any standards nor a budget for cooperation with universities. Thus, all existing contacts and cooperation are informal'. 'Funding, staff size and availability of specialized academic personnel' to assist with public safety efforts were

seen as necessary to improve outcomes, particularly ‘increased funding for research into forensic tools and analysis, and training and skilled personnel’. Despite the need for ‘More resources and openness in law enforcement, and more applied research in academia’, significant potential exists for expanded cooperation with government institutions and law enforcement authorities.

11. Prevention and Protection of Cyber-crime via technology

Crime prevention’ refers to the strategies and measures that seek to reduce the risk of Crimes occurring, and their potential harmful effects on individuals and society, though interventions that influence the multiple causes of crime. The United Nations Guidelines for the Prevention of Crime highlight that government leadership plays an important part in crime prevention, combined with cooperation and partnerships across ministries and between authorities, community organizations, non-governmental organizations, the business sector and private citizens. Besides that the people have to use to with the recent technological benefits to reduce cyber-crime. Some of the technological supports to prevent cyber-crimes are given below. Firewalls monitor traffic between your computer or network and the Internet and serve as a great first line of defense when it comes to keeping intruders out. Make sure to use the firewall that comes with your security software. And if you have a home wireless network, enable the firewall that comes with your router.

When you're checking your email or chatting over instant messenger (IM), be careful not to click on any links in messages from people you don't know. The link could take you to a fake Website that asks for your private information, such as user names and passwords, or it could download malware onto your computer. Even if the message is from someone you know, be cautious. Some viruses replicate and spread through email, so look for information that indicates that the message is legitimate. When navigating the Web, you need to take precautions to avoid phony Websites that ask for your personal information and pages that contain malware. Use a search engine to help you navigate to the correct Web address since it will correct misspellings. That way, you won't wind up on a fake page at a commonly misspelled address. (Creating a phony site at an address similar to the real site is called "typo squatting," and it is a fairly common scam.)
Use comprehensive security software and keep your system updated because hackers have a wide variety of ways to access your system and information, you need comprehensive security software that can protect you from all angles. Software can help protect you from malware, phishing, spyware, and other common and emerging threats. Just make sure that you keep your security software up-to-date by selecting the automatic update function on your security control panel. And don't forget to perform regular scans. You also want to update your operating system (OS) and a browser with the latest security patches. If you are a Microsoft Windows® user, you can enable automatic updates to keep your OS safe.

11.1. Secure your wireless network

Hackers can access data while it's in transit on an unsecured wireless network. You can keep the hackers out by enabling the firewall on your router and changing the router administrator password. Cybercriminals often know the default passwords and they can use them to hack into your network. You may also want to set up your router so it only allows access to people with passwords that are encrypted. Check your owner's manual for instructions on setting up encryption.

11.2. Use Strong Passwords

Although it may be easier for you to remember short passwords that reference your birthday, middle name, or pet's name, these kinds of passwords also make it easy for hackers. Strong passwords can go a long way in helping secure your information, so choose a password that is at least 10 characters long and consists of a combination of letters, numbers and special characters. Also consider changing your password periodically to reduce the likelihood of it being compromised.

11.3. Use Common Sense

Despite the warnings, cyber-crime is increasing, fueled by common mistakes people make such as responding to spam and downloading attachments from people they don't know. So, use common sense whenever you're on the Internet. Never post personal information online or share sensitive information such as your social security number and credit card number. Exercise caution when clicking on any links or downloading any programs.

11.4. Be Suspicious

Even if you consider yourself cyber savvy, you still need to keep your guard up for any new tricks and be proactive about your safety. Backup your data regularly in case anything goes wrong, and monitors your accounts and credit reports to make sure that a hacker has not stolen your information or identity. Although protecting yourself does take some effort, remember that there are a lot of resources and tools to help you. And by adopting a few precautions and best practices, you can help keep cybercrime from growing.

12. Conclusion

To fight cyber-crime we must not impose all liabilities to the government. Computer and internet system facilitated the non-government organizations a lot. They have the largest interest in cyber security. At several of US national institute of Justice revealed that the business and financial institutions comprises 46 percent of computer crime targets while the government comprise only 8 percent of the targets. So, non-government

organizations must come forward to augmenting the governmental initiatives with money. Logistics and specialized manpower. The Mumbai cyber lab is a unique initiative of police public collaboration for training police officers in the investigation of cybercrime. Similar initiates have also been taken by other states of India. Bangladesh should follow their suit. The government should welcome outsourcing initiatives to prepare a galaxy of virtual police officers and establish few cyber police stations across the country as soon as possible. Those cyber-crime fighters should be given specialized training home and abroad. The non-government organizations utilizing computers and internet system, as their means of business operation should sponsor to send the virtual police officers abroad for advanced training on cybercrime prevention and investigation.

Reference

1. APEC Leaders Statement on Counter-terrorism, APEC Economic Leaders' Meeting, Shanghai, 21 October 2001.
2. APEC, Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cyber security Strategy, 2002/CSOM/052, Concluding Senior Officials Meeting, Los Cabs, B.C.S., Mexico, 21-22 October, 2002.
3. Cybercrime Expert Group, Proposal, Doc No: telwg29/ESTC/12, APEC Telecommunications and Information Working Group, 29th Meeting, 21-26 March 2004, Hong Kong, China.
4. Cybercrime Expert Group, Proposal, Doc no: telwg29/ESTC/12, APEC Telecommunications and Information Working Group, 29th Meeting, Hong Kong, China, 21-26 March 2004
5. Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA II), Chapter V.
6. ICT, act 2006.
7. The copy right act, 2000
8. The telegraph Act 1885.
9. The sale of goods Act-1930
10. Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986. Cited in UN, Crimes related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, A/CONF. 187/10
11. G7 conference about prevention of cyber-crime, Chairman's Statement, 17 June 1995, Halifax Summit, and 15-17 June 1995.
12. G8, Okinawa Charter on Global Information Society, Okinawa, 22 July 2000.
13. Brenner Susan, Cyber Crime: Criminal threats from cyber-crime PRAEGER 2010, pg 23

14. Collins, huge *the law of contract*4th, London: lexis nexis butterworths, 2003.

15. Kevin Mitnick history is taken from these sources, Cyberpunks, Katie Hafner and John Markoff and Cybercrime, Burner, Susan W.

16. Md. Abu hanif, Mass media and cyber laws of Bangladesh.2014

17. The ICT act, 2013 (amended)

18. Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean, Kingston, Jamaica, 3-7 November, 2003, published in January, 2004.

19. Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean, Kingston, Jamaica, 3-7 November, 2003, published in January, 2004.

20. Against organization, http://nailart-online-studio.blogspot.com/2012/02/cyber-crime-assignment-oum 1.html

21. Cyber-crime against property, http://nailart-online-studio.blogspot.com/2012/02/cyber-crimeoum-semester-1.html

22. Dimension of cyber-crime, http://www.slideshare.net/faridahusin/ cyber-crimes-for-oumh1203

23. http://www.lawyersnjurists.com/articles-reports-journals/science-and-technology/cyber-crimes-bangladesh