International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 23-09-2019; Accepted: 26-10-2019
www.lawjournals.org
Volume 5; Issue 6; November 2019; Page No. 129-134

Cyber-crime investigations issues and challenges

Dattatray Bhagwan Dhainje
Cyber expert, Advocate, Bar council India, Pune, Maharashtra, India

Abstract
The facilities of computer technology have not come out without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber-crime' without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber-crimes and their impacts over various areas like Sochi-eco-political, consumer trust, teenager etc. with the future trends of cyber crimes are explained.

Computer crime is the use of information technology in any suspicious criminal activities. Recently, our life becomes increasingly depending on modern information technology; however, it becomes very important to improve the computer crime investigation procedure especially in cases of processing very important and sensitive information such as government and military intelligence, banking information or personal private information. Cybercrime investigation helps detecting unauthorized access to any digital source information with the intent of modifying, destroying or stealing that digital data or information. Such suspicious actions can cause financial damages or important information loss; moreover, it might distribute or destroy high secret and private or confidential information. Therefore, this paper focuses mainly on highlighting the main challenges of the Indian States (Maharashtra, Karnataka, Delhi and Hyderabad) in computer crime investigation system by taking a look at the recent developments in the continent's Internet infrastructure and the need of information security laws in these particular countries.

Over the past ten years, crime (traditionally based in the world of physical entity) has been increasingly making its way into the world of information. Crime is evolving; since the days when goods were transported by stagecoach, robbery has changed to keep up, even to our modern-day equivalent-credit and debit cards. Internet credit card number theft has become a well-recognized danger. The most common forms of computer crime reported to Inter -GOV include child pornography, fraud, and e-mail abuse. Even more disturbing are new forms of cyber-terrorism made possible by the large amount of the physical machinery now operated by computers. In this article, after attempting to define computer crime, we examine the types that have been committed in the past, and the new types likely to appear in the future. We also examined the difficulty in detecting and measuring computer crime, methods for attempting to prosecute or prevent such crimes, and the effectiveness of these measures. This article evaluates the concepts of computer crimes, detection and the controls. The paper finally exposed us to dangers it poses to organizations, factors that encourage it, and recommending possible controls and preventive measures against computer crimes.

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cybercrime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds.

The present study has been undertaken to touch some aspects, effect and prospects of this cyber-technology with special reference to threat poses of Cybercrime by India. Efforts have been made to analyze legal framework available for its control in India. To start with, it is, therefore, necessary to demarcate the dimensions of word 'crime'. Thus it is beyond doubt that 'crime' is a relative phenomenon, universal in nature and essentially all societies from ancient to modern have been evidently demonstrating its presence. Each society have been providing its own description of criminal behavior and conduct made punishable by express will of the political community ruling.

Over the society and it was always influence by religious-social-political economical values prevailing in the given society. Thus from time immemorial the behavior that attracts '*penal liability*' influenced and characterized by overall outcome of these standards. Parenthetically, just as concept of crime [has undergone] change with the growth of Information Technology so the categories of criminals who engage in such crimes. So far Indian society is concerned, particularly during ancient period, the definition of crime flagged by religious interpretation. The period was known for complete dominance of religion. All political and social activities in general and 'Crime' in particular, considered to be happened due to the presence of super-natural power. The Demonological theory of crime causation was an outcome of this period. Due to the revolution of communication and information technology the use of internet has been enlarged which increases the rate of digital crime all over the world. Digital crime can be defined as "crimes directed at digital devices or their application systems." It is very important to secure sensitive information that are processed over the web (Internet) such as government and military intelligence, banking information or personal private information. Nowadays, our life becomes increasingly depending on modern information technology; however, it becomes very important to improve the computer crime investigation procedure especially in case of processing very important and sensitive information. Computer crimes may include different suspicious activities such as machine unauthorized access, digital frauds, system interference as well as computer misuse which might not involve any type of machine physical damage. In fact, computer crime is not just unauthorized access to a computer system with intent to delete, modify or damage computer data and information but it's so far more complex. It can be any type of information. The purpose of this paper is therefore to highlight the main challenges of the Indian States (Maharashtra, Karnataka, Hyderabad and Delhi) in computer crime investigation system, by taking a look at the recent developments in the continent's Internet infrastructure and the need of information security laws in these particular countries.

Keywords: Sochi-eco-political, cyber-crime, security laws, stagecoach etc

1. Introduction
1.1 Significance of Cyber Crime Investigation
The purpose of the ITU report Understanding Cybercrime: Phenomena, Challenges and Legal Response is to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks. As such, the report aims to help developing countries better understand the national and international implications of growing

cyberthreats, to assess the requirements of existing national, regional and international instruments, and to assist countries in establishing a sound legal foundation

1.2. Scope of Cyber Crime Investigation [1]:

Understanding the Scope of the Investigation

As mentioned, there are three basic types of investigation. With each type, the rules get tighter and the consequences of failure to comply get progressively stricter. A good rule of thumb is to pretend that the strictest rules apply to all investigations. However, as you might imagine, there are some role-specific requirements that don't apply to all of them.

Internal Investigations

Internal investigation is the least restrictive of the inquiries you might make. From a standpoint of professional courtesy, internal investigations are more likely to be the least hostile type you'll ever do. You work directly with management, and the target of your inquiries probably won't even be aware of your activities until you are finished. You don't have courts and lawyers combing every word you say or write, hoping to find the smallest mistake.

That is not to say that there aren't laws that apply to internal probes. There most certainly are. State and federal laws regarding privacy apply to even the smallest organization. Also, different states have different laws regarding how companies deal with employment matters, implied privacy issues, and implied contracts. This isn't intended to be a law book, so for the purposes of brevity and clarity, understand this. It is important to review any relevant regulations before you make your first move.

Most corporations have formal guidelines for such matters. In addition to a written employee handbook, it is very likely that a company has documented guidelines regarding issues leading to termination, use of company infrastructure (including computers, e-mail systems, and network services), and so forth. In every step of your process, make sure that you adhere to the law and to corporate policy. If there appears to be a conflict between the two, get legal advice. At the very least, make sure you have written authorization to perform every step you take. Management needs to be aware of your process and every step involved in the course of investigation, and they must sign off, giving approval. Document everything you do, how you did it, and what results you obtained. In digging into the source and impact of any internal security breach, your foremost concern is the protection of your client. However, should your probe uncover deeper issues, such as illegal activity or a national security breach, then it becomes necessary to call in outside authorities?

Civil Investigations

Civil cases are likely to be brought to the organization in situations where intellectual property rights are at risk, when a company's network security has been breached, or when a company suspects that an employee or an outsider is making unauthorized use of the network. Marcella and Menendez (2008) identify the following possible attacks:

- Intrusions
- Denial-of-service attacks
- Malicious code
- Malicious communication
- Misuse of resources

An investigator involved in a civil dispute should be cognizant of the Federal Rules of Civil Procedure. Although a legal degree is hardly necessary, a strong background in civil law is invaluable. Additionally, experience in business management is useful, in that a good understanding of standard corporate policy is necessary. Good communications skills are required. Management needs to be able to feel equally comfortable dealing with a CEO or a secretary.

When working with large repositories of data connected too many different users and devices, it becomes more difficult to assess who actually committed an infraction. Proving that a specific user was accessing the network at a specific time (and possibly from a particular machine) can be critical to winning a case. Anson and Bunting (2007) point out the difficulties of generating an accurate **timeline** and recommend some good tools for simplifying the matter. A good manager will keep abreast of changing technology and make sure that the organization is equipped with the proper tools.

Tools required for examining large networks or performing live data capture are substantially more expensive than those used to search individual data sources. Generally, it is not possible to bring down a corporate network while the investigative team captures images of thousands of drives. Costs in time and materials would be prohibitive, as would be the negative impact of downtime on the company. Specialized software is needed to capture, preserve, and document the data. Additional tools are needed for data reduction. Filtering out the general network chatter and unrelated business documents can be a time-consuming process.

Keeping up with newer technology is essential, as is constant refresher training. The organization must continually assess its current capabilities and apply them to what imminent future needs are likely to be. As technology advances, investigative tools and techniques need to advance as well. Cases are won and lost on the ability of investigators to extract evidence. If a forensics team finds itself faced with a technology it doesn't understand, there will be no time for on-the-job training.

Criminal Procedure Management

Defining precisely what constitutes computer crime is very difficult to do. Fortunately, it is not up to the investigator to determine what is and what not criminal activity is. However, some definitions have been presented by various experts. Reyes (2007) states that a computer crime will exhibit one or more of the following characteristics:

- The computer is the object, or the data in the computer are the objects, of the act.
- The computer creates a unique environment or unique form of assets.
- The computer is the instrument or the tool of the act.
- The computer represents a symbol used for intimidation or deception.

[1] http://ijcsit.com/docs/Volume%204/Vol4Issue5/ijcsit2013040519.pdf,

Generally speaking, computer crimes are little different from conventional crimes. Somebody stole something, somebody hurt somebody else, somebody committed fraud, or somebody possessed or distributed something that is illegal to own (contraband). While not an exhaustive list of possible computer crimes, the following is a list of the most commonly investigated:

- Auction or online retail fraud
- Child pornography
- Child endangerment
- Counterfeiting
- Cyberstalking
- Forgery
- Gambling
- Identity theft
- Piracy (software, literature, and music)
- Prostitution
- Securities fraud
- Theft of services

Prosecution of criminal cases requires a somewhat different approach than do civil cases. Legal restrictions are stricter, and the investigator is more likely to be impacted by constitutional limitations regarding search and seizure or privacy. Failure to abide by all applicable regulations will almost certainly result in having all collected evidence suppressed because of technicalities. Many civil investigations are not impacted as severely by constitutional law because there is no representative of the government involved in the investigation. To assure that the investigation succeeds, management of a criminal division needs to have someone with a strong legal background. Courts will use the Federal Rules of Evidence to decide whether or not to allow evidence to be admitted in an individual case.

For the same reasons, reporting procedures and chain of custody must be rigorously followed by each person involved in an investigation, whether they are involved directly or peripherally. Even a minor departure from best practice is likely to be challenged by opposing counsel. Because of this, selection of personnel becomes a greater challenge. A technical whiz with little or no documentation ability is likely to fail in criminal investigation. Anyone who demonstrates a disregard for authority is a poor candidate for investigating criminal cases.

Tools used in criminal cases are subject to a tighter scrutiny than those used in civil cases. When a person's life or liberty hangs in the balance, judges and juries are less sympathetic to a technician who cannot verify that the tools used to extract the evidence being presented are reliable. Software and hardware tools used by the organization must be recognized by the court for use, and the techniques used by investigators must be diligently documented to show there was no deviation from accepted standard procedures.

Funding is likely to be more limited in criminal work than in civil investigations. Money will be coming from budget-strapped government entities or from law offices watching every dime. In some cases, courts will apply the Zubulake test to determine if costs should be shifted from one party to the other. This test is based on findings from the case *Zubulake v. UBS Warburg* (217 F.R.D. at 320, 2003) where the judge issued a list of seven factors to be considered in ordering discovery (and in reassigning costs). These factors are to be considered in order of importance, the most important being listed first:

1. The extent to which the request is specifically tailored to discover relevant information
2. The availability of such information from other sources
3. The total cost of production compared to the amount in controversy
4. The total cost of production compared to the resources available to each party
5. The relative ability of each party to control costs and its incentive to do so
6. The importance of the issues at stake in the **litigation**
7. The relative benefits to the parties of obtaining the information

1.3 Statement of the Research Questions

Following questions have been stated as follows:

1. What are the provisions relating to Cybercrime Investigation?
2. Who are the persons involving in Cyber Crime Investigations?
3. Issues and challenges of Cyber Crime Investigation?

1.4 AIMS and Objective of Research

The Researcher would like to put forth aims and objectives of the given topic as per own Individual understanding and expect a radical change in Cyber Crime Investigations. The following shall be the aims and objectives of the given subject.

The objective of the India Cybercrime Centre will be to coordinate various efforts pertaining to cybercrime prevention and regulation in India. It aims to provide assistance to law-enforcement agencies and contribute to the fight against cybercrime in India. It will also aim to act as a centre for the emerging cybercrime jurisprudence that is evolving in India. The India Cybercrime Centre will also engage in providing training and capacity building amongst the various stakeholders. It is expected that the India Cybercrime Centre will be the focal point in Indian efforts against cybercrime. It will also aim to primarily provide more distinct approaches on how to deal with emerging cybercrimes. It would also aim to support various law enforcement agencies in India at the Central and State level in building legal capacity for detection, investigation, and prosecution of cybercrimes as also for cooperation with various international players.

The India Cybercrime Centre will aim to develop the evolving jurisprudence on cybercrimes and also will aim to look at all kinds of cybercrimes which are targeted against persons, property or nations.

One of the objectives of the India Cybercrime Centre is to empower the users of Internet in India. They would able to be more sensitized about the emerging trends on cybercrime. Cybercrime today is evolving as part of our day-to-day lives. Cybercrime is an hourly phenomenon and therefore legal mechanisms and strategies have to be appropriately so as to deal with emerging challenges on cybercrime.

The India Cybercrime Centre will also engage in research and development of emerging cybercrime jurisprudence that is happening worldwide and how the same could be made applicable in the context of the Indian ecosystem.

The India Cybercrime Centre would also be engaging in capacity building and contributing to trainings on legal and policy issues pertaining to cybercrime and what strategies

need to be adopted by the law-enforcement agencies in going forward in the detection, investigation and prosecution of cybercrimes.

It is expected that the India Cybercrime Centre will aim to contribute the fight against cybercrime in India.

The objectives include

1. To promote the idea that the competent practice of computer forensics and awareness of applicable laws is essential for today's networked organizations.
2. To help managers understand how computer forensics fits as a strategic element in overall organizational computer security.
3. To enlighten the mass on issues associated with computer forensics. iv. To embark on a product awareness and campaign to leverage cybercrime.

1.5. Statement of Hypothesis

In the light of the research following Hypothesis is formulated:

- Cyber Crime Investigation rate is less so conviction rate is also less.

1.6. Research Methodology

The method adopted for doing this research is doctrinal research. The researcher mainly emphasized on the different kinds of emergency, and has given a little more emphasis on the effects of emergency and various other related things. Have also taken references related to our topic, and have given more emphasis to the substantive part of our research work, and have also referred to some of the official websites and articles.

1.7 Review of Literature

The Researcher has Relied on various Primary and Secondary Sources including Judicial Pronouncements IT ACT 2000,IT ACT 2008 Amendment, Indian Evidence Act 1872 and other Legislations and criminal Procedure Code and various reference books written by Prof.Jyoti Ratan and Prof,Farooq Ahamad.

1.8 Limitataion of Research

The researcher would like to limit the research of cyber-crime investigation and its applicability in India. The limitation of the research would be to study the effect of Cyber Crime Investigation its Issues and Challenges.

Cases

In a bid to increase detection and conviction rate of cyber-crimes in the state and the city, the Mumbai police have organised five days cyber-crime training workshop for policemen and have setup a specialsed cyber-crime investigation units at each police station in Mumbai.

According to the statistics provided by Maharashtra Police, the state Police has an extremely poor conviction as well as detection rate in Cyber-Crime cases. Statistics shows that since 2012, on an average, almost 80 % of the cases results in acquittal of accused. The poor conviction rate only raises questions over the investigation techniques adopted and evidences gathered by the police department in probing Cyber-Crime cases.

From 2012 till June 2017, trial in 184 cyber-crime cases got completed, of which there were convictions in 34 cases and acquittals in 150 cases, statistics revealed.

Baba Ramdev's Patanjali to step into solar power business, will invest Rs 100 crore

According to the statistics, the detection rate of Cyber Crime cases is only 31% in last five-and-a-half years. Out of 10,419 cases registered under Information Technology Act along with Indian Penal Code and Special law cases, since year 2012 till June 2017, only 3167 cases have been detected.

While registration of Cyber-Crime cases have increased from 900 cases in 2012 to 2417 in year 2016, the detection rate has fallen from 33.3 percent in 2012 to 23.07 in the year 2016.

AirAsia tickets in Rs 999: deal details you need to know

Also the pendency of Cyber-Crime cases in court is on the higher side. As per the statistics, 10,235 Cyber-Crime cases are still pending in the court.

Cyber experts and cybercriminal lawyers said that lack of proper training and poor investigation skills leads to poor conviction rate and detection rate. "Electronic evidence requires to be collected and processed expeditiously and in a manner which stands the test of trial. Inordinate delay in either collection or forensic analyses will adversely affect the legality and proving of such evidence. The forensic cyber lab in Mumbai is grossly over worked and hence forensic analysis and reports are much delayed in many cases. In addition, delays in registration of cases and in investigations by the police irreparably harm effective decisions in cases," said N. S. Nappinai, advocate and author specialising in cyber laws.

Paytm ka ATM is here! Firm plans to invest Rs 3000 crore over next 3 years to expand offline distribution network

"Sometimes complainants also delay filing of complaints - this may be due to either confusion with respect to rights available with them or lack of confidence in the system. That the number of cases filed does not reflect the actual cyber-crimes committed is probably a reflection of this! Each of the above may be contributory factors resulting in the abysmally low convictions," Nappinai added.

"Since police is unable to gather sufficient evidences in such cases, it results in poor conviction. There is a need for special cyber-crime courts to fast track the cases. Also the quality of training should be upgraded. There is load on forensic lab too and report is delayed there. Even citizens

Chap 2: Cyber Crime Investigations Challenges and Solutions

[2]. The threat from cyber-crime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate. Cyber-criminal tools pose a direct threat to security and play an increasingly important role in facilitating most forms of organized crime and terrorism.

Challenge 1

There is now a sophisticated and self-sufficient digital underground economy in which data is the illicit commodity. Stolen personal and financial data – used, for example, to gain access to existing bank accounts and credit

[2] https://www.inc.com/lolly-daskal/10-smart-leadership-solutions-for-every-challenge.html

cards, or to fraudulently establish new lines of credit – has a monetary value. This drives a range of criminal activities, including phishing (the act of attempting to acquire information such as usernames, passwords, and credit card details and sometimes, indirectly, money, by masquerading as a trustworthy entity in an electronic communication), pharming (the fraudulent practice of directing Internet users to a bogus Web site that mimics the appearance of a legitimate one), malware distribution and the hacking of corporate databases, and is supported by a fully-fledged infrastructure of malicious code writers, specialist web hosts and individuals able to lease networks of many thousands of compromised computers to carry out automated attacks.

Solutions [3]

Active targeting of underground fora to disrupt the circulation of powerful and easy to use cyber-criminal tools, such as malware kits and botnets.

Disrupt the infrastructure of malicious code writers and specialist web hosts through the active identification of developer groups and a joint action of law enforcement, governments and the Information & Communication Technology industry to dismantle so-called "bullet proof" hosting companies.

Active targeting of the proceeds of cyber-crime in collaboration with the financial sector. For e.g. money mule (is a person who transfers money acquired illegally (e.g., stolen) in person, through a courier service, or electronically, on behalf of others) [4].

Continue to develop insight into the behavior of the contemporary cyber criminal by means of intelligence analysis, criminological research and profiling techniques, and based on the combined law enforcement, IT security industry and academic sources, in order to deploy existing resources more effectively.

Challenge 2

In the last decade advances in communications technologies and the "information" of society have converged as never before in human history. This has given rise to the industrialization of a type of crime where the commodity, personal information, moves far too quickly for conventional law enforcement methods to keep pace.

The unprecedented scale of the problem threatens the ability of the authorities to respond with millions of viruses and other types of malicious code are in global circulation, and again innumerable computers are compromised per day At the same time, the authorities have more data on criminal activity at their disposal than ever before, and now have an opportunity to harness this information in ways which make intelligence development and investigation more streamlined and cost effective.

Cyber crime rates continue to increase in line with Internet adoption: mobile Internet access and the continuing deployment of broadband Internet infrastructure throughout the world therefore introduces new levels of vulnerability; with potential victims online for longer periods of time and capable of transmitting much more data than before; and the increasing trend for outsourcing data management to third parties presents imminent risks to information security and data protection.

Solutions

More must be done to harness the intelligence of network and information security stakeholders, not only to provide a more accurate and comprehensive assessment of cyber criminality, but also to ensure that responses are effective and timely. Active partnerships are to be made with ISPs, Internet security organizations and online financial services are keys.

Collaboration, particularly with the private sector, to proactively identify features of future communications technologies liable to criminal exploitation, and to design vulnerabilities out of technologies and environments which are in development.

Challenge 3

[5] Cyber crime is a truly global criminal phenomenon which blurs the traditional distinction between threats to internal (criminality and terrorist activity) and external (i.e. military) security and does not respond to single jurisdiction approaches to policing. The liability of networks to exploitation for a number of different ends, and the ease with which individuals may move from one type of illegal activity to another suggests that territorialism in all its forms (both of nations and regions, and specific authorities within nations) hinders efforts to successfully combat the misuse of communications technology.

At present, national authorities are overcoming jurisdictional restrictions by coordinating regionally or with agencies with similar levels of capability/capacity to better understand and respond to Internet-facilitated crime.

Solutions

More centralized coordination at regional and interregional levels, to streamline the fight against cyber crime.

Global Cyber Law should be implemented.

The establishment of virtual taskforces to target Internet facilitated organized crime. These should be responsive to the evolving criminal environment – e.g. more permanent groups for information sharing, more ad hoc arrangements for specific operations such as dismantling botnets. In all cases the authorities need to have the flexibility to include a variety of stakeholders (law enforcement, military, and private sector, and academia, user groups) in order to achieve the desired outcome. One of the virtual task force can be World Cyber Cop.

The World Council for Law Firms and Justice promotes the evaluation and harmonization of the legal systems throughout the world. There are many small and many great steps on the road to fulfilling this vision. This consideration of ideas on the establishment of an International Court for Cyber Crime is intended as the start of an international initiative to mark an important milestone on the long road.

The establishment of an International Cyber Criminal Court (comprising of highest level of Judicial Authority and Technical Authority) for the prosecution of Internet crimes

[3] https://www.sciencedirect.com/science/article/pii/S0263237313001576

[4] http://w3.siemens.com/smartgrid/global/en/about-siemens-smart-grid/challenges_and_solutions/pages/challenges-and-solutions.aspx

[5] http://www.halliburton.com/en-US/ps/solutions/heavy-oil/heavy-oil-challenges-and-solutions.page

could wholly or partially reduce the criminals' lead. The realization of this vision requires expertise, commitment and courage – including the courage to ignore borders and to think consistently towards the future.

There should be a World Tribunal which should control all the Country Courts which in turn should have many Regional Tribunals.

Challenge 4

Another most alarming problem in the present day cyber world is the promotion and easy availability of pornography especially Child pornography which refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a child. Abuse of the child occurs during the sexual acts which are recorded in the production of child pornography.

Solutions

Place the computer in a centrally located area in your home - not in a child's bedroom. This prevents "secret" communications or access and also allows all members of the family to use it. Talk to your children about the Internet. Explain that it is an excellent source of information, but some sites are inappropriate and they are expected to stay away from these sites. Establish time frames for Internet access. This will encourage your children to obtain information in a timely manner and discourage aimless wandering. Keep an open line of communication with your children. Discuss their Internet experiences and guide them to sites that are age-appropriate. Consider using software that can block or filter Internet sites or certain words that may indicate inappropriate sites.

In a chat room never give out any personal information including: name, address, city, state, school attended, telephone number, family names or other personal family information. Never respond to someone who wants to meet in person or send photographs. Instruct your children to exit the chat room and notify you immediately if this happens. Most importantly, if your child visits a particular chat room, spend at least five or ten minutes monitoring the conversation to see if it is appropriate. Consider purchasing computer software products that an help you monitor and control your child's access to the Internet. Monitor your children's Internet activity by checking all of the sites visited

Chap 3: Measures to Prevent Cyber Crimes [6]

Know How To Recognize Phishing. Your bank won't send you an email telling you that your account has been compromised and asking you to provide sensitive account and personal information like password, PIN etc. it already has. These are obviously phishing attempts.

Recognize that your Smart-phone is really a pocket-size computer and is prone to the same types of attacks directed at your laptop and desktop. Take steps to protect it, such as keeping your operating system current and creating a strong password.

Keep your personal information to yourself. For instance, don't put your entire birth date, including the year, on Facebook. Think about the security questions normally posed by your bank and other secure locations: "first school you attended," "name of favorite pet" and the like.

Know the pitfalls of public Wi-Fi. CreditCards.com says, "Avoid public wireless Internet connections unless you have beefed-up security protection."

Beware of public computers, too. For instance, Kiplinger says, "Don't access your accounts or personal information on public hotel computers, which could have software that logs keystrokes and records your passwords and account numbers."

Use credit cards, rather than debit cards, when making purchases online. In case of fraud, you'll get much better protection from liability with a credit card.

Purchase only from reputable websites [7] (and look for "https" in the Web address). "It is really easy to create a fake online store or to create a store that sells stuff, but its real purpose is to collect credit card information," former identity thief Dan DeFelippi told CreditCards.com.

Check your accounts and your credit reports regularly. Some experts recommend that you check bank account and credit card activity every day. You can pull a free credit report every four months from AnnualCreditReport.com to verify that fraudulent accounts have not been created in your name.

[8] Avoid suspicious E-mails. Don't click on links in suspicious emails, even those that appear to be from friends. Emailed viruses and malware are the most prevalent cyber threat of identity theft. Just think of how many emails you've gotten in the last year that appeared to be from friends whose email accounts were hijacked.

Chap 4: Conclusion and Suggestions

Although the main theme of this group workshop was "Challenges and Best Practices in Cybercrime Investigation", it is not always possible to discuss such issues without venturing into the debate about legal frameworks, given that most procedural tools designed to overcome the challenges and some implementations of best practices need to be supported by proper legislation within each country. Nevertheless, the group worked to identify common issues and strived to reach consensus on the recommendations towards the improvement of the fight against the threat of cybercrime. Whenever possible, those recommendations were included in the main body of this document, immediately following the discussion of the respective subject for the sake of clarity and conciseness.

The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious. The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programs will only affect a percentage of possible victims. The others need to be automatically protected through measures that do not stress and require considerable participation. Security needs to be easy and effective if it is doing work. Whether cybercrime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of cybercrime will be proportional to real-world crimes.

9. References

1. Cyber Law Books by Pavan Duggal
2. Cyber law in India: (law on internet) / by Farooq Ahmad.
3. Cyber Law and Information Technology by Dr.Jyoti Ratan
4. "Cyber Warfare: A Multidisciplinary Analysis (Routledge Studies in Conflict, Security and Technology)" by James A Green

[6] https://www.huffingtonpost.com/toby-nwazor/5-ways-to-prevent-cyber-c_b_12450518.html

[7] http://cybertimes.in/?q=node/540

[8] https://mumbaimirror.indiatimes.com/mumbai/other/12-ways-to-protect-yourself-from-cyber-crime/articleshow/20025280.cms?prtpage=1