August 2, 2010

CYBER CRIME IN PRESENT WORLD

AMIT GUPTA, Dr.

Available at: https://works.bepress.com/amit_gupta/1/
INTRODUCTION:

Crime:

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment.”

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

Cyber Crime

A generalized definition of cyber crime may be “unlawful acts wherein the computer is either a tool or target or both” Cyber crime is the latest and perhaps the most complicated problem in the cyber world. “Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime”. “Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime”

How cybercrime work – and makes money

Cybercrime has become a profession and the demographic of typical cybercriminal is changing rapidly, from bedroom-bound geek to the type of organized gangster more traditionally associated with drug-trafficking, extortion and money laundering.

It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin (and with far less risk), the only time the criminal need leave his Personal Computer is to collect his cash. Sometimes they don’t even need to do that.

The rise of cybercrime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency. Cybercrime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.

The probable marketplace for the transaction of cyber criminals will be a hidden IRC (Internet Relay Chat) chat room. The fees for providing information, sharing skills will most likely be exchanged in some form of virtual currency such as e-gold.
Cybercriminals can be categorized as –

Coders – Comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, ‘coders’ produce ready-to-use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cybercrime labour force – the ‘kids’. Coders can make a few hundred dollars for every criminal activity they engage in.

Kids – So-called because of their tender age: most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, php mailers, proxies, credit card numbers, hacked hosts, scam pages etc. ‘Kids’ will make less than $100 a month, largely because of the frequency of being ‘ripped off’ by one another.

Drops – The individuals who convert the ‘virtual money’ obtained in cybercrime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent ‘safe’ addresses for goods purchased with stolen financial details to be sent, or else ‘safe’ legitimate bank accounts for money to be transferred into illegally, and paid out of legitimately.

Mobs – Professionally operating criminal organizations combining or utilizing all of the functions covered by the above. Organized crime makes particularly good use of safe ‘drops’, as well as recruiting accomplished ‘coders’ onto their payrolls.

Various types of Cyber Crime

1. Unauthorized access to computer systems or networks / Hacking-

This kind of offence is normally referred as hacking in the generic sense. Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information which is critical in nature.

2. Cyber Stalking

Cyber Stalking can be defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Stalking in general terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker.
Both kind of Stalkers “Online & Offline” – have desire to control the victims life. Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim’s immediate family; and still others require only that the alleged stalker’s course of conduct constitute an implied threat. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously.

**How do they Operate**

a. Collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. He collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

b. The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.

c. People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

d. Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

e. Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.

f. In online stalking the stalker can make third party to harass the victim.

g. Follow their victim from board to board. They “hangout” on the same BB’s as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will “flame” their victim (becoming argumentative, insulting) to get their attention.

h. Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

i. Contact victim via telephone. If the stalker is able to access the victims telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.

j. Track the victim to his/her home.

**Nature and Extent of Cyberstalking**

Online harassment and threats can take many forms; cyberstalking shares important characteristics with offline stalking. Many stalkers – online or offline – are motivated by a desire to exert control over their victims and engage in similar types of behavior to accomplish this end. In many cases, the cyberstalker and the victim had a prior
relationship, and the cyberstalking begins when the victim attempts to break off the relationship. However, there also have been many instances of cyberstalking by strangers. Given the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes.

The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. Put another way, whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence.

3. Denial of service Attack

This is an act by the criminal, who floods the bandwidth of the victim’s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide

Denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DOS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DOS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DOS attacks are constantly being dreamed up by Hacker.

4. Virus / worm attacks

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. For eg. the VBS_LOVELETTER virus (better known as the Love Bug or the Iloveyou virus) was reportedly written by a Filipino undergraduate.

The original VBS_Loveletter utilized the addresses in Microsoft Outlook and emailed itself to those addresses. The e-mail, which was sent out, had "Iloveyou" in its subject line. The attachment file was named "Love-Letter-Foryou. TXT.vbs". The subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file conquered people wary of opening e-mail attachments. The message in the e-mail was "kindly check the attached Loveletter coming from me".
In May 2000, this deadly virus beat the Melissa virus hollow - it became the world's most prevalent virus. It struck one in every five personal computers in the world. When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10 billion.

Since the initial outbreak over thirty variants of the virus have been developed many of them following the original by just a few weeks. In addition, the Love Bug also uses the Internet Relay Chat (IRC) for its propagation. It e-mails itself to users in the same channel as the infected user. Unlike the Melissa virus this virus does have a destructive effect. Whereas the Melissa, once installed, merely inserts some text into the affected documents at a particular instant during the day, VBS_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever-increasing versions of itself. Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

5. Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

6. Trojan attacks

A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. There are many simple ways of installing a Trojan in someone's computer. For eg. ‘A’ sends spoofed e-cards to ‘B’ which appears to come from third persons account. The e-card actually contained a Trojan. As soon as ‘B’ opened the card, the Trojan was installed on his computer. ‘A’ now had complete control over B’s computer and proceeded to harass him thoroughly.

7. Internet time thefts

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In a case reported before the enactment of the Information Technology Act, 2000 in India Colonel Bajwa, a resident of New Delhi, asked a nearby net café owner to come and set up his Internet connection. For this purpose, the net café owner needed to know his username and password. After having set up the connection he went away with knowing the present username and password. He then sold this information to another net café. One week later Colonel Bajwa found that his Internet hours were almost over. Out of the 100 hours that he had bought, 94
hours had been used up within the span of that week. Surprised, he reported the incident to the Delhi police. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber crimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested the net café owner under the charge of theft as defined by the Indian Penal Code. The net café owner spent several weeks locked up in Tihar jail before being granted bail.

8. Web jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website. In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

9. Data Diddling-

This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed.

10. Salami attacks-

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. the Ziegler case wherein a logic bomb was introduced in the bank’s system, which deducted 10 cents from every account and deposited it in a particular account.

11. Email bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the 169 schemes was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of
mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

The Cyber crimes, which can be committed against the followings group

1. Against Individuals: –

   i. Harassment via e-mails.
   ii. Cyber-stalking.
   iii. Dissemination of obscene material.
   iv. Defamation.
   v. Unauthorized control/access over computer system.
   vi. Indecent exposure
   vii. Email spoofing
   viii. Cheating & Fraud

2. Against Individual Property: -

   i. Computer vandalism.
   ii. Transmitting virus.
   iii. Netrespass
   iv. Unauthorized control/access over computer system.
   v. Intellectual Property crimes
   vi. Internet time thefts

3. Against Organization: -

   i. Unauthorized control/access over computer system
   ii. Possession of unauthorized information.
   iii. Cyber terrorism against the government organization.
   iv. Distribution of pirated software etc.

4. Against Society at large: -

   i. Pornography (basically child pornography).
   ii. Polluting the youth through indecent exposure.
   iii. Trafficking
   iv. Financial crimes
   v. Sale of illegal articles
   vi. Online gambling
   vii. Forgery
Cyber Laws Worldwide Position

To meet the challenge posed by new kinds of crime made possible by computer technology including telecommunication, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. Some of these countries are USA, Austria, Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore. However, no country has fully resolved all the issues such as legal, enforcement and prevention of crime. The legislations enacted by different countries cover only few of the classified computer related offences. However, looking to the dynamic and fast changing technology, new types of offences may pop-up frequently.

Cyberlaw has been a vibrant field in which numerous developments took place in the year 2001 on the global level. It is not fair to undermine the importance of some events as compared to others since each development in the field of Cyberlaw was a step further towards a more definitive, regulated and orderly cyberspace and towards evolving the regulated code of conduct for online activities in the context of electronic medium.

The first most important development that took place in the field of Cyberlaw in the year 2001 on the global scenario was one event, which substantially altered the rules of the game in the prickly issue concerning jurisdiction. This was the Yahoo! France case.

From the beginning of Internet, jurisdiction has continued to challenge legal minds, societies and nations in the context of the peculiar inherent character of the Internet.

Different principles were being evolved in different national jurisdictions in this regard. In the beginning the courts of different countries began making the mere access to Internet as a sufficient ground for assuming jurisdiction over Internet related transactions. Then that principle got a substantial redefinition by the Zippo case in the United States of America. The Zippo case required courts to look at something more the mere Internet access in order to assume jurisdiction. That “something else” could be in the form of the interactivity of the website or any other factor. The year 2001 saw a further redefining of the principles of the important subject of jurisdiction in the famous Yahoo! France case.

This case has a peculiar history. Two groups in France complained to the court that Yahoo! France’s auction websites sold Nazi memorabilia and Third Reich related goods, which is banned under French Law. They consequently requested the court to take stringent action. Yahoo! took up the plea that it was a company incorporated in the United States of America and that the French Laws did not bind it. It was further contended that, technologically speaking, it was not possible for Yahoo! to block access to all Nazi Memorabilia.

The French Court ordered Yahoo! France to remove all Nazi memorabilia and content from its website failing which it would have to pay a fine of 100,000 franc for each day of non-compliance. Yahoo! complied with the order of the French Judge and remove almost all of the Nazi memorabilia links on its auction sites.
However, Yahoo! also moved an American court for a declaration that the directions given by the French Judge were not enforceable in United States and that Yahoo! being an American company was not bound by the decision of the French Court.

In a historical judgment, the American District Court of California held that the directions of the French Judge could not be enforced in the United States of America, as the same were violative of the first Amendment of the US Constitution. The Judge further held that though the American court respected the French judgment, yet the fact was that the French judgment was passed in the peculiar facts relating to France and that such judgment would not be applicable in American Law on American citizens and legal entities.

This judgment has got far reaching significance and consequences on the entire subject of jurisdiction. Till now, the courts anywhere in the world could assume and were assuming jurisdiction on Internet transactions and websites that were located outside the country.

This decision underlines the principle that even if a foreign court passes a judgment or direction against a legal entity of a particular country say Country A, then that judgment or direction would not be applicable automatically to country A’s legal entity or citizen. The decision or direction of the foreign court will need to be scrutinized by country A’s courts keeping in mind the touch stone and basic principles enshrined in the constitution of the country as also enshrined in the local laws of that country, before it can be enforceable in Country A.

This judgment should also deter courts on unnecessarily assuming jurisdiction on Internet related matters. Even the Zippo principle has been further redefined by Yahoo judgment. For these particular reasons, I personally consider this is to be one of the two most important developments, which took place in the field of Cyberlaw in the year 2001.

The second most important development in the field of Cyberlaw in this year relates to cyber crime, September 11th attacks on the World Trade Center and the consequent signing of the International Cyber Crime Treaty. Since the beginning of Internet, cyber crime has been emerging as a major source of headaches for government all across the world. The absence of any international law on cyber crime further complicated matters with different countries assuming distinct national approaches for controlling, regulating and preventing cyber crime.

September 11th 2001 saw the turning point in the history of the World Wide Web and the Internet. The attacks on World Trade Center’s Twin Towers were an example of how terrorist acts had been conceived, planned and committed using the means of Internet. That singular instance of September 11th changed the way we use the Internet and the way Internet is going to be regulated.

The scenario emerging post September 11th 2001 saw the adoption of the International cyber crime Treaty. This international treaty, being a baby of the European Union, was adopted after 29 drafts and more than 4 years of work. 30 members of the European Union apart from the United States, Canada, South Africa and Japan have already signed the International Cyber crime Treaty.
The International Cyber Crime Treaty promises to become the first international benchmark for controlling and regulating cyber crime and for ensure cooperation amongst different signatory nations for exchanging information concerning cyber crime and cyber criminals. The International Cyber Crime Treaty is yet to come into implementation. However, almost single handedly the treaty promises to fill up the void about the need for having an international regulatory mechanism for controlling cyber crime that has existed since the beginning of Internet.

The International Cyber Crime Treaty also becomes the first international treaty to be in place for any issue concerning Cyberlaw. The treaty may not be perfect, and no treaty is perfect. However it does give a very strong starting point for international efforts to regulate and control cyber crime. This treaty also promises to possibly change the way cyber crime would be investigated, regulated and punished on a global scenario, in the context of increasing cooperation and exchange of information between signatory member countries on the issue of regulating cyber crime. This has been the second most important development in the field of Cyberlaw.

**Suggestions for evading scams**

One should not respond to spam. If you reply, even to request removing your e-mail address from the mailing list, you are confirming that your e-mail address is valid and the spam has been successfully delivered to your inbox. Lists of confirmed e-mail addresses are more valuable to spammers than unconfirmed lists, and are frequently bought and sold by spammers.

Check to see if the e-mail address is visible to spammers by typing it into a Web search engine. If your e-mail address is posted to any Web sites or newsgroups, remove it if possible to help reduce how much spam you receive. Disable in-line images, or do not open spam messages. Frequently spam messages include "Web beacons" enabling the spammer to determine how many, or which e-mail addresses have received and opened the message. Most current e-mail programs disable in-line images by default to prevent this from occurring.

One should not click on the links in spam messages, including unsubscribe links. These frequently contain a code that identifies the e-mail address of the recipient, and can confirm the spam has been delivered and that you responded.

When unsubscribing from e-mail, the main rule to follow is: if you didn't originally opt-in to receive it, or if you don't recognise the sender / company sending the e-mail, then don't unsubscribe. Trying to unsubscribe from one e-mail can start a flood of mail from other sources, so if you are unsure, it is best not to unsubscribe and block the mail another way. When unsubscribing from mail always check that the links in the e-mail go to the correct company Web site and not a Phishing site. When filling in Web forms, one has to check the site's privacy policy to ensure it will not be sold or passed on to other companies. There may be a checkbox to opt out of third party mailings.

One should not respond to e-mail requests to validate or confirm any of your account details. Your bank, credit card company etc. already have your account details, and would not need you to validate them. If you are unsure if a request for personal
information from a company is legitimate, contact the company directly or type the Web site URL directly into your browser.

One should not click on the links in the e-mail, as they may be fake links to phishing Web sites.

If you have an e-mail address that receives a large amount of spam, consider replacing it with a new address and informing your contacts of the new address. Once you are on lots of spammers' mailing lists, it is likely that the address will receive more and more spam.

**General guidelines on Cyber Safety**

Do not give out identifying information such as your name, home address, or telephone number in a chat room. Even vital details like age, gender should never be divulged to anyone.

Do not send your photograph to any one on the net unless you know the person well enough.

Do not respond to messages or bulletin board items that are obscene, belligerent or threatening.

Never arrange a face-to-face meeting with someone who you have just ‘met’ on the Internet. In case you have to meet this person, make sure you have someone with you for the meeting. And inform someone of the person and place you will be going to. Remember, people online are not always who they seem to be.

**Virus Warnings** Virus warnings are a very common occurrence in the mail box. While one shouldn’t take these warnings lightly, a lot of times, such warnings are hoaxes and will do more harm than good. Always check the story out by visiting an anti-virus site such as McAfee, Sophos or Symantec before taking any action, including forwarding them to friends and colleagues.

---

**Corporates can make their businesses secure by following these simple guidelines:**

- Setup an e-security program for your business
- Ensure your security program facilitates confidentiality, integrity and availability
- Identify the sources of threats to your data from both internal and external sources. Examples: disgruntled employees - leaving bugs behind in your system, hackers looking to steal confidential information.
- The security program that you create for your business must have provisions to maintenance and upgrades of your systems
• Administrators have access to all files and data. Therefore, one must be mindful of who is guarding the guards
• Roles for security should be defined, documented, and implemented for both your company and external contractors.
• Establish a security awareness program for all users. Content should be communicated in non-technical terms. This could include briefings, posters, clauses in employee contracts, security awareness days etc
• Implement security training for technical staff that is focused on the security controls for their particular technical areas
• Maintain logs of all possible activities that may occur on your system. System records must note who was using the system, when, for how long, deletions etc.
• User accounts should not be shared. User authorization should be mandatory. Employees should only be able to see information that they are authorized to see.
• Employee user accounts must be disabled or removed when no longer needed. Example: in case an employee leaves the company.
• Ensure network security from external sources by installing firewalls and intrusion detection systems.
• Allow remote access to employees only through secure communication channels like SSL or VPN
• Install antivirus software on all desktops and servers. Buy Anti-Virus software solutions that allow real time upgrading of systems with anti-virus patches.
• Create a data backup and disaster recovery plan in case of unforeseen natural calamities.
• Ensure back-up procedures are in place and tested
• Ensure back-up procedures include all your critical as well as back office data such as finance, payroll etc.
• Incident response is the ability to identify, evaluate, raise and address negative computer related security events.
• Incase of an incident, do not panic, and continue to save logs.
• Incident response - Take a backup of the affected system and notify the authorities.

**Guidelines for Personal Computer**

Home computers are as susceptible as office computers to online attacks. Here are some extremely important guidelines for home computer owners.

1. Use the latest version of a good anti-virus software package that allows updating from the Internet.
2. Use the latest version of the operating system, web browsers and e-mail programs.
3. Don't open e-mail attachments unless you know the source. Attachments, especially executables (those having .exe extension) can be dangerous.
4. Confirm the site you are doing business with. Secure yourself against "Web-Spoofing". Do not go to websites from email links.
5. Create passwords containing at least 8 digits. They should not be dictionary words. They should combine upper and lower case characters.
6. Use different passwords for different websites.
7. Send credit card information only to secure sites.
8. Use a security program that gives you control over "Cookies" that send information back to websites. Letting all cookies in without monitoring them could be risky.

Use a firewall

We strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks. However, no firewall can detect or stop all attacks, so it’s not sufficient to install a firewall and then ignore all other security measures.

One should never open an unknown email attachments

Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs.

If you must open an attachment before you can verify the source, we suggest the following procedure:

1. Be sure your virus definitions are up-to-date
2. Save the file to your hard disk
3. Scan the file using your antivirus software
4. Open the file

For additional protection, you can disconnect your computer's network connection before opening the file. Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.

Don’t run programs of unknown origin

Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing - they might contain a harmful program.

Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.
Disable Java, JavaScript, and ActiveX if possible

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Turning off these options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some web sites.

Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites.

Why one should report cyber crime

Crime in a society is expected to remain at a tolerable level due to the deterrence factor; early detection of the crime, identification of the criminal who has committed the crime and awarding of an exemplary punishment to him/her will dissuade other individuals who would have indulged in such instances in future. An unreported crime emboldens the criminal to commit further such acts, apart from taking away the deterrence for others. Proper reporting also helps policy makers to know of the trends and allocate resources to adequately tackle newer crimes. Critical infrastructure protection, which has an impact on a large number of people also benefits by having proper reporting practices.

You may be worried about the loss of reputation or negative publicity; however, most law enforcement organizations are aware of this and take steps to keep crime details confidential. They also are sensitive to the fact that the reporting company's business may depend on the availability of the computer resources involved and can take appropriate measures to use forensic tools to ensure that business disruption is minimized. There have been numerous important developments, which have impacted Cyberlaw in these years. Suffice it is to say at this juncture Cyberlaw is constantly developing, it is expected that the coming years are likely to see further consolidation in the growth of the Cyber Law as an evolving discipline.