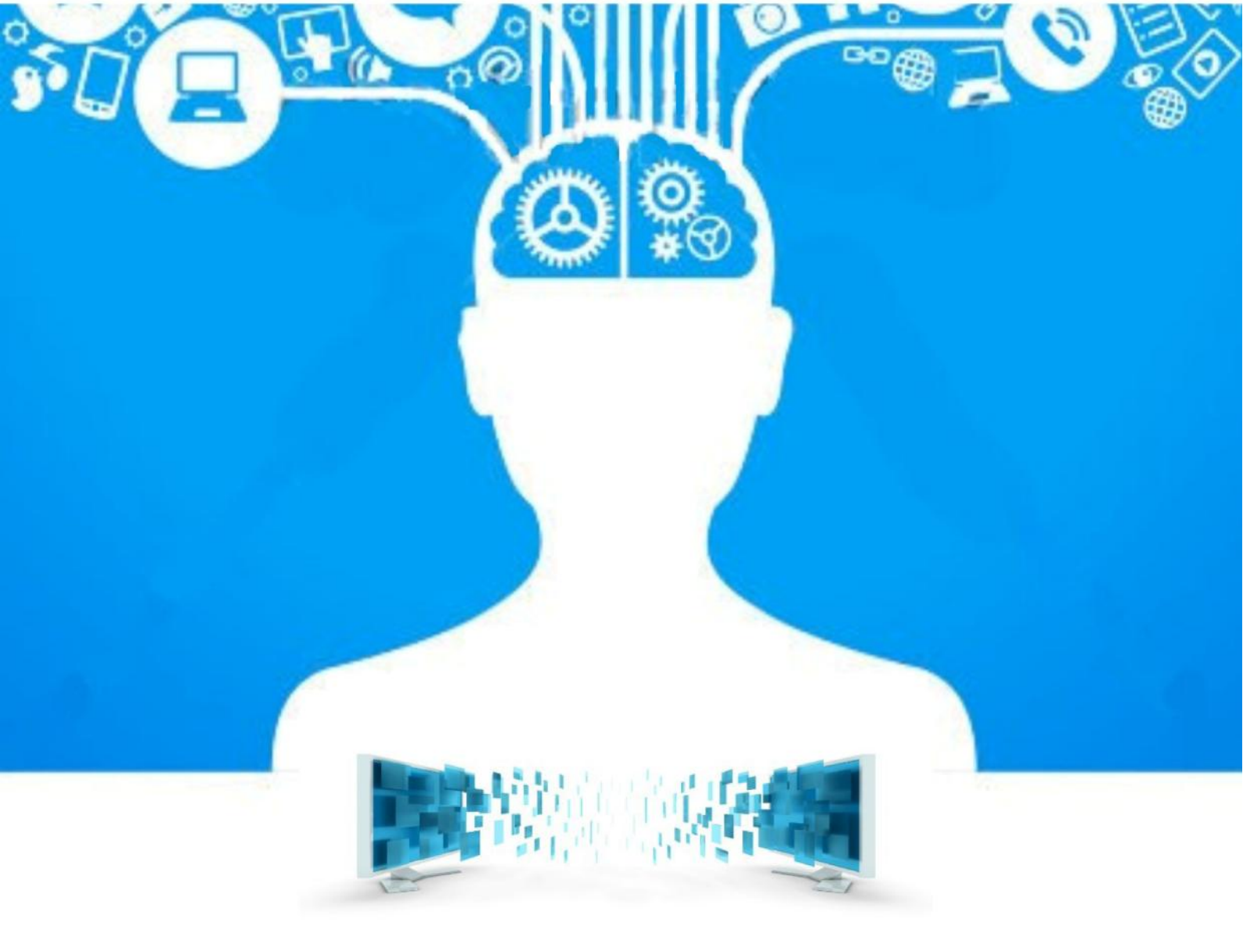
LORETO
COLLEGE

IN-HOUSE JOURNAL

I.C.T
SOCIETY
EIGHTH EDITION
2014-2015

CONNECT



Note from the Principal's Desk

Information Communication and Technology (ICT) continues to take the world by storm and has revolutionized communication. A useful and progressively important means of bringing the world closer and a service to humanity, ICT has transformed lifestyle and lives.

In this day, with the advancement of Information and Technology, and with competition creeping in – competition to be better than the others, to have more than the others, to know more than the others – cyber-crime is on the increase. An awareness of Information Security and the need to guard this, is what is portrayed in 'Connect' 2015.

Congratulations to the ICT Society President, Nidhi Baid, Vice-President, Sudarshana Sinha, Staff Advisors, Ms. Chandrani Sengupta and Ms. Swati Chatterjee, for putting together this issue of 'Connect'.

Sr. Christine Coutinho
Principal, Loreto College

Note from the Staff Advisors

Information and Communications Technology necessitates its users to know the current and emerging skills around computing and communications devices, software that operates them, applications that run on them and systems that are built with them. However, there is a need to know how to use all the features provided by ICT in a safe manner without getting compromised with regard to privacy of personnel information, maintaining secrecy of information and creating trust in the computing environment.

Significant increase in cyber-attacks and cybercrimes have exposed users to misuse of information, cyber bullying, sexual exploitation etc. Therefore, it was the endeavor of the ICT Society to make the users understand the risks/impact of cybercrime or cyber-attacks, a step towards building a secure information society.

The enthusiasm of the contributors with the intent to widespread the awareness help us to publish the Eight edition of our In-house journal “CONNECT” about the cyber threats associated with unsafe use of Internet.

Ms. Swati Chatterjee
Ms. Chandrani Sengupta

Note from the Editor’s Desk

All of us from the ICT Society would just like to say what a pleasure it was working on this magazine and how grateful we are for receiving this opportunity to learn so much about the topic "Cyber Crimes and Hacking", not only from the research put into it, but also from each and every article we received.

We would like to thank our Staff Advisers, Ma'am Sengupta and Ma'am Chatterjee for being with us every step of the way.

Nidhi Baid, President
Sudarshana Sinha, Vice President
Naomi Chatterjee, Treasurer

SAVING ONESELF FROM NET CRIME

In this day and age computers and internet are a very important part of our life. We tend to rely on computers a lot; doing most of our work via these sources .However we should also be aware about the importance of cyber security and protect our computers from cybercrime or net crime as it is commonly known as, it refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. There are certain counter measures which can be taken to protect oneself from cybercrime these include: technical measures like installing a firewall and an antivirus in our computers or cryptography techniques can also be employed to encrypt information. Behavioral countermeasures such as becoming more aware about the whole process can be an effective tool in combating cyber-crime, which is becoming a major threat in today's world.

SANJANA VIJ
1ST YEAR, POLITICAL SCIENCE, (H)

INTERNATIONAL MEASURES TO FIGHT AGAINST CYBERCRIME

With new advances in the field of information technology, it has been seen that information dissemination and most importantly, communication, has become a transnational activity. Cyber space has become boundary less and has united all parts of the world globally.

Though the advantages and the uses of this cyber field are numerous; one cannot overlook the misuse of information technology either. In fact, cybercrime is an emerging issue right after social crime and terrorism. It would not be wrong to say that cyber-crime is used as a tool to promote terrorist activities too. Some of the most common types of such crime are hacking, fraud mails, heat messages, and the like. The emergence of various social networking sites has provided an additional impetus to the growth of cyber-crime all over the world. Thus we can demarcate the aspects of cybercrime into two distinct levels- Individual and National.

Individual cybercrime can still be avoided if one is aware of such trends and do not engage into attractive offers via mail; or keep their documents and passwords protected from external handlings or viruses. The problem comes with the ongoing trends of National cyber-crime. With hacking and interception of communication, state Secrets and various domestic and diplomatic information falls in wrong hands. This information can be later misused and become the reason for large scale violence.

The immediate question that now arises is that whether measures are being taken against combatting cyber-crime or not. Much before common man started asking this question the heads of various Nations asked the same. That is exactly why this trans-national crime has become a very serious subject of deliberations and time and again conferences and meets are held between various representatives of the Nations wherein measures and preventions are discussed and adopted. Some of the most renowned of such conferences are:

- The discussions taking place in the united nations in various instances during 1990, 2000 and again in 2002. The main topic of the deliberations undergoing in such UN meets were resolutions against dealing with criminal misuse of information technology. The UN was one of the primary institutions that recognised the need to look into the matter of cyber- crime.

- The G8 which is a group of eight countries comprising US, UK, Russia, France, Italy, Japan, Germany and Canada have also taken up cyber- crime as one of its serious agendas during the 1997 meets. The Ministers Communique, an action plan against cyber- crime was formulated. It laid down the principles of law enforcement against this type of crime. Most importantly, it realised the need to train personnel’s in effectively combatting cyber- crime.

- The council of Europe in 2001 met at a convention on cybercrime. There were 46 Member States who signed the provisions against these crimes but only 25 countries ratified the principles of the conventions later on.

- Another effective meeting was undertaken by the International Telecommunication Union in 2003. The Geneva declaration of Principles or the Geneva Plan of Action laid profound guidelines dealing with the importance of fighting cybercrime.

- In recent times, the cooperation between The United States of America and China -which also happens to be the two highest victims of Cyber- crime -has given a new dimension of awareness of these crimes to the whole world.

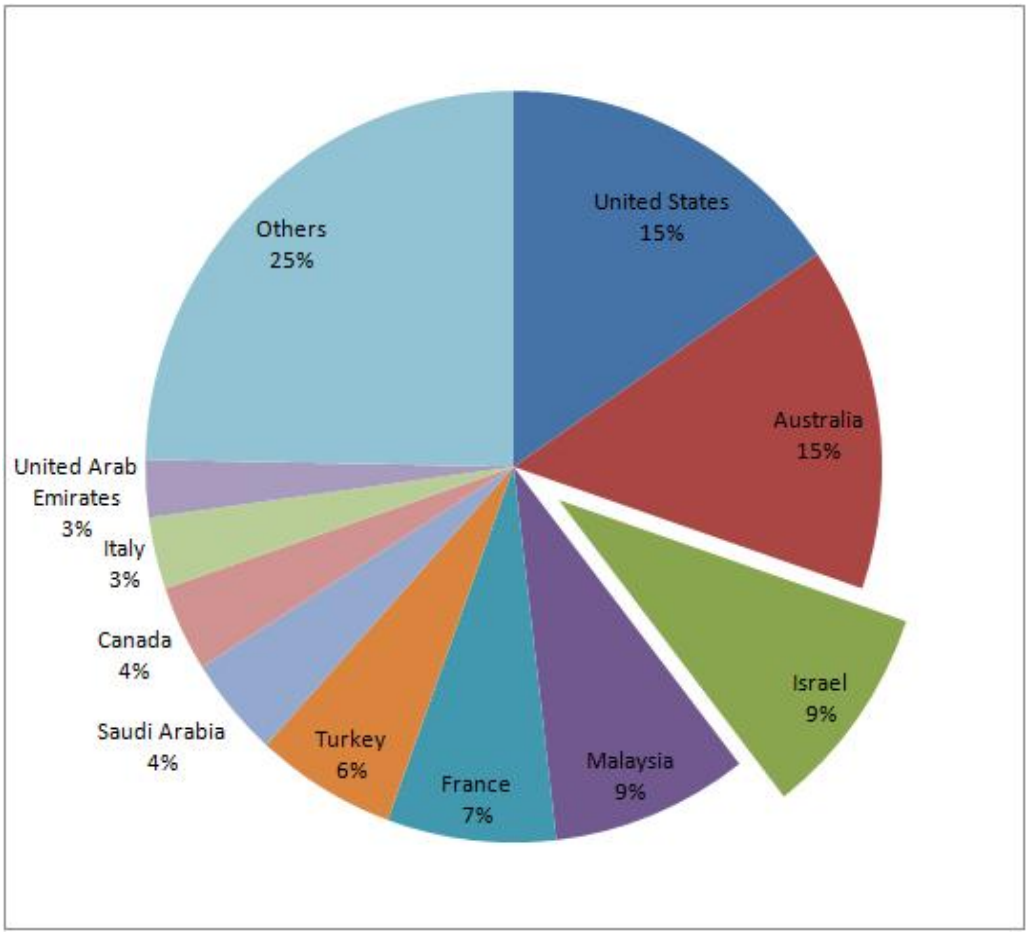
  What needs to be understood here is that any measures taken against cyber-crimes face two very distinct oppositions. First, it becomes very difficult to trace these cyber criminals as they are extremely intelligent and there is lack of personnel training in identifying such criminals all over the world. Second, it is a great challenge in itself to be able to judiciously enforce laws against such cyber criminals. There are certain National and International Laws existing against cyber -crimes; but the actual challenge is using them in the appropriate moment for the appropriate cause.

  Thus, the need of the hour today is not to just be aware of cyber -crime but to be able to apply our awareness at the right time. In doing so one might be able to do great service to the society.

SUBHADRIKA SEN
3RD YEAR, POLITICAL SCIENCE (H)

FACT FILE

COUNTRIES AFFECTED BY CYBER CRIME



FACTS ABOUT CYBER CRIME AND HACKING

FIRST RECORDED CYBER CRIME.

- The first cyber crime ever recorded was In France during 1820.
- The person involved was Joseph-Marie Jacquard.
- He was a textile manufacturer, he made looms.
- He invented looms that can store designs.

Hackerspeak

Hackers – white and black hats – have their own language. Here are few examples of amusing, amazing hacker lingo

Brute force attack

A hacking method used to find passwords or encryption keys by trying combinations of characters until the correct one is found

Camping out

A hacking technique of breaking into a system and finding an undetected place to monitor the system, store information, or re-enter the system at a later time

Dropper

This executable file, when run, drops a virus or Trojan on a computer system. A dropper file intends to create a virus or Trojan and then execute it on the user's system

Ham

Non-spam messages

Exploit

To use the defects found in software code or function on a system to elevate privileges, execute code remotely, cause denial of service, or prompt other attacks.

In the wild

The state of a virus when two independent researchers identify it in circulation within a one-year period. Approximately 450 viruses exist in the wild at any given time.

Logic bomb

Also called time bomb, a program that allows a Trojan to lie dormant and then attack when conditions are just right.

Warhol Worm

The concept that a computer virus can spread around the world in less than 15 minutes. Based on Andy Warhol's idea that every individual will have 15 minutes of fame.

Ping attack

The method of overwhelming a network with ping commands.

Zoo Virus

A virus found only in virus laboratories that has not moved into general circulation.

Spit

A type of spam conveyed via VoIP

Source: MacAfee Threat Glossary

CYBER CRIME BYTES

BANGALORE accounts for 24.4 per cent of cyber crimes booked under the IT Act among 53 'megacities' across India.

CITY TOPS national charts with 342 cyber crime cases booked in 2012, up from 117 in 2011

KARNATAKA RANKS third in the country with 412 cyber crime cases

registered in 2012. Bangalore accounts for approximately 83 per cent cases being booked in the State

OF 412 cyber crime cases, 323 under IT Act or IPC in Bangalore fall under 'loss/ damage to computer resource' and 'hacking'.

Source: National Crime Records Bureau

SUDARSHANA SINHA
3RD YEAR, GEOGRAPHY (H)

CYBO GLOOM

The facilities of computer technology have not come out without drawbacks. Though it makes the life speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as “CYBERCRIME” where without computers entire businesses and government operations would almost cease to function. A good measure of changing trends in the computer industry is changes in cyber criminal behavior. The post PC era is clearly here-and it is already looking to be a more dangerous era with the acceleration of cyber attacks against mobile devices, social media platforms and Macs in the past year. Moreover cyber criminals continue to enhance their tools to improve the effectiveness of cyber attacks.

Identity theft, financial fraud, website defacements and cyber bulling are some common examples of cybercrime. Further, at an organization level, cybercrime may involve the hacking of databases and theft of intellectual property or confidential information along with sniffing network traffic and virus dissemination. African countries like Kenya, Nigeria, Tunisia, Tanzania etc. are almost free from the cyber laws and policies, whereas major cyber crimes reported in India are denial of services, defacement of website, SPAM, Computer virus, Pornography, Cyber Squatting, Cyber Stalking and phishing.

Therefore education and lectures alone cannot help in eradicating cyber nuisance. The only appropriate way to fight them is by enacting new laws, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies.

DEBARUPA GHOSH
1ST YEAR, GEOGRAPHY (H)

CYBER-CRIME AND CYBER-SECURITY

Cybercrime or Computer crime has been defined by experts as an offence 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 modern telecommunication devices like computer, mobile phones, internet etc. Such crimes may even threaten national security and finance. Internationally, both governmental and non-state actors engage in cybercrimes- including espionage, financial theft and cross-border crimes. Interpol has said that it is making the war against cybercrime its main priority.

Computer experts have identified several ways to fight cybercrimes-

1. Using strong complicated passwords, one for each account.
2. Securing one's computer or mobile device by activating firewalls and using anti-virus software to block spyware attacks.
3. Being careful while sharing information on social networking sites and reviewing the shared information.
4. Securing wireless networks and avoiding the use of public networks.
5. Being cautious while giving out personal information such as one's name, address, phone number or financial information etc.
6. Thinking before clicking on links or files of unknown origin.
7. Arranging for regular maintenance for telecommunication devices.
8. Reporting immediately in case of any computer-related crime.

CYBER INFERNO

Technology is a constantly changing entity, perpetually evolving and always progressing. Cyber crime, or computer crime, entails the use of a computer, a device which has seemingly become indispensible to the human race, as an instrument to further illegal ends.

In layman terms, most cyber crimes stem from the existence of metaphorical lock and key; the key symbolizing the various illicit means by which our privacy insecurity are threatened in the virtual world and the lock representing our progressively futile attempts to safeguard against such intrusions.

Amongst the most broadly classified cyber crimes feature financial crimes, defamation, online gambling, cyber stalking, web jacking, cyber pornography, etc.

Defenders of an information system can use a variety of counter measures depending on the nature of the attack and the availability of resources. To briefly list a few such measures:

1. **EDUCATION**: This involves awareness of operating procedures, the key attack targets (like passwords) and the classic attack methods.

2. **ENCRYPTION**: Encryption hides information in some form that cannot be easily read; one must supply a character-string “key” to decode it when needed.

3. **DECEPTION**: Systems could lie and mislead attackers to prevent them from achieving their goals.

4. **PATCHES**: Many manufacturers provide “patches” or “security updates” to remedy flaws in newly released software in the form of modified software that one must subsequently download. Software that has been available for a significant period of time generally requires fewer patches because such inherent flaws are eventually found and fixed. Thus, purchasing just released software products is not a good idea.

5. **INTRUSION DETECTION AND COMPUTER FORENSICS**: Intrusion Detection Systems (IDSs) can be installed to check and record events that might indicate an attack, alerting system administrators when matters turn serious. For new and complex attacks, Computer Forensics is required for inspecting how the attack was accomplished and the damage it left behind.

Other measures include the use of **Access Controls**, **Honeypots, Backtracking**, and of course **legal measures**.

In this context, it must be mentioned that since many such cyber-attacks destroy data or programs, making copies or "backups" of digital information is essential to recovery from any attack.

The lack of powerful general counter general measures means that attacks on computer systems and networks will continue to rise in the future. Certain measures like Patches, Encryption, Intrusion Detection, Computer Forensics, Backtracking, Deception and Honeypots will certainly prove useful in the future as technical details concerning their implementation are worked out.

In conclusion, however, it must be said that the present day counter measures do help protect systems as they raise the necessary level of sophistication required by an attacker to succeed.

The title **CYBER INFERNO** is illustrative of the misery that cyber-crime leaves in its wake. The term "inferno" meaning hell, is an apt choice, for portraying the hellish experience of individuals caught in this vice.

SACHIKA GHOSH
1ST YEAR, HISTORY (H)

CYBER ATTACKS...

Cybercrime is a crime committed using a computer or internet to steal a person's identity or illegal imports or malicious programs. In other words, it is nothing but where computer is used as a subject or object of crime. The first recorded cybercrime took place in 1820! This is not surprising since abacus, which is considered to be the first form of computer, has been around since 3500 B.C.

Cybercrimes can be categorized in two ways-

- **The computer as a target-** to attack other computer like hacking, virus attacks etc.
- **The computer as a weapon-** to commit real world crimes like Cyber Terrorism, Credit Card Frauds, Pornography etc.

Types of cybercrime-

- **Hacking**
- **Child Pornography**
- **Denial of Service Attack**
- **Virus Dissemination**
- **Computer Vandalism**
- **Cyber Terrorism**
- **Software Privacy**

In today's world where everything from small gadgets to nuclear plants is being operated through computers, cybercrime has assumed threatening ramifications. There is a huge potential of damage to national security through cyber-attacks. The internet is a means of money laundering and funding terrorist attack in an organized manner.

Cyber Security involves protection of sensitive personal and business information through prevention, detention and response to different online attacks.

Advantages of Cyber Security-

- Cyber Security will defend us from critical attacks.
- It helps us to browse safe websites.
- It processes all the incoming and outgoing data on our computer.
- It will defend us from hacks and viruses.
- The security developers will update their database every week. Hence, any new virus is also deleted.

Challenges of Cyber Security-

- Explosion of Computer and broadband internet availability.
- Low priority of security for software developers.
- Challenge of timely patching vulnerabilities on all systems.

Safety tips to Cyber Crime-

- Use of antivirus software.
- Insert firewalls.
- Uninstall unnecessary software.
- Maintain back up.
- Check security settings on a regular basis.

PAULAMI DE
1ST YEAR, GEOGRAPHY (H)

CYBER TERRORISM

“An underworld don is hospitalized for a minor surgery. His rival goons hire a computer expert to hack into the hospital's computer systems and alter the medicines prescribed for the don. The nurse unknowingly gives the don a high dose of the medicine, to which the patient is severely allergic, resulting in his death.” This was the first ever cyber murder reported in the US five years ago. Cybercrime is a modern day crime, committed via computers. Its emergence can be traced to the rapidly evolving technological systems of the 21st century.

Cyber-crime has reached gigantic proportions today as everything from the Televisions and Air-conditioners to nuclear power plants is being run on computers. Today, the world is moving towards a point where everything from banking stock exchanges, are traffic control, telephones to electric power, health care, welfare and education depends on software. This exponential growth, and the increase in the capacity and accessibility of computers coupled with the decrease in cost, has brought about revolutionary changes in every aspect of human civilization, including crime.

The difference and major advantage of a cyber-crime from crimes of any other nature is that it is committed in a virtual space, by proxy, but has consequences and effects that are far reaching and real. And because they are committed by proxy, there is a sense of security and anonymity that the perpetrator feels shrouded, enabling an entire spectrum of offenders to resort to cybercrime. The spectrum includes idealists like the teenagers who commit it as a novelty crime, most often attacking entire systems with viruses they created; the greedy who target e-banking and commerce with the specific intention of making money and are well rehearsed in escaping law-enforcement; and the cyber terrorists. They are the newest and most dangerous group. Their primary motive is not just money but also a specific cause they defend.

The threat of cyber-terrorism can be compared to those of nuclear, bacteriological or chemical weapon threats. This disheartening issue is that they have no state frontiers; can operate from anywhere in the world, and this makes it difficult for them to get caught. The types of cyber crimes include pornography, cyber fraud, defamation, cyber stalking, harassment, data hostage, money laundering, phishing, e-mail bombing, cyber war etc.

General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act, 2000 was passed. This Act was a welcome step at a time when there was no legislation on this field. The Act has however during its application proved to be inadequate and there are certain loopholes in the Act. Cyber Crime in the Act is neither comprehensive nor exhaustive.

The Information Technology Act has not dealt with cyber nuisance, cyber stalking, and cyber defamation and so on. Cases of spam, hacking, stalking and e-mail fraud are rampant although cyber crimes cells have been set-up in major cities. The problem is that most cases remain unreported due to lack of awareness. Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space. However, it is quite possible to check them. But we can win only through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy.

NISHAT FATIMA KHAN
1ST YEAR, EDUCATION (H)

CYBER CRIME AND IT'S EFFECTS

What is cyber crime?

Computer crime**,** or Cybercrime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. **Net crime** is criminal exploitation of the Internet.

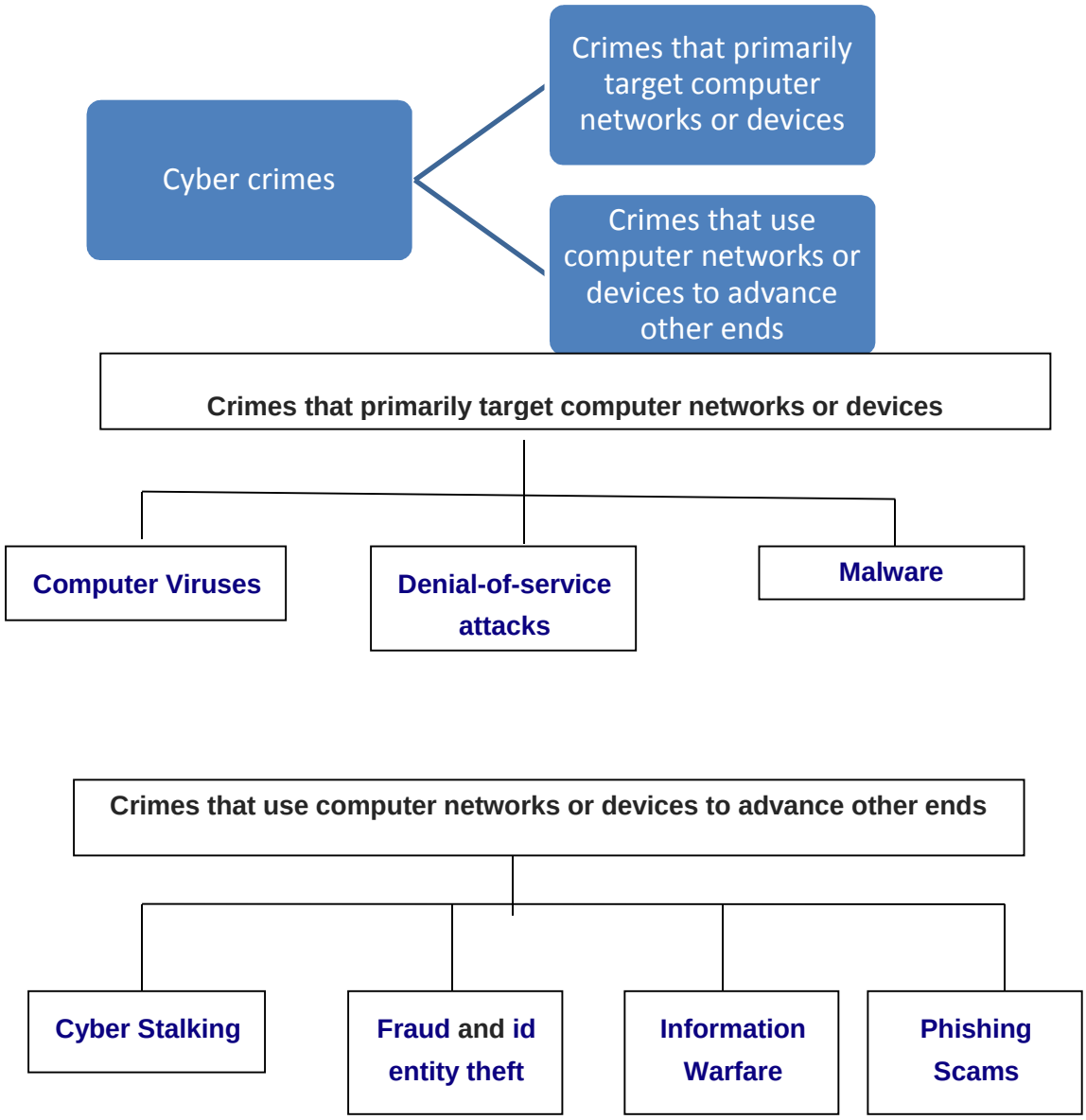
Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".Such crimes may threaten a nation's security and financial health.

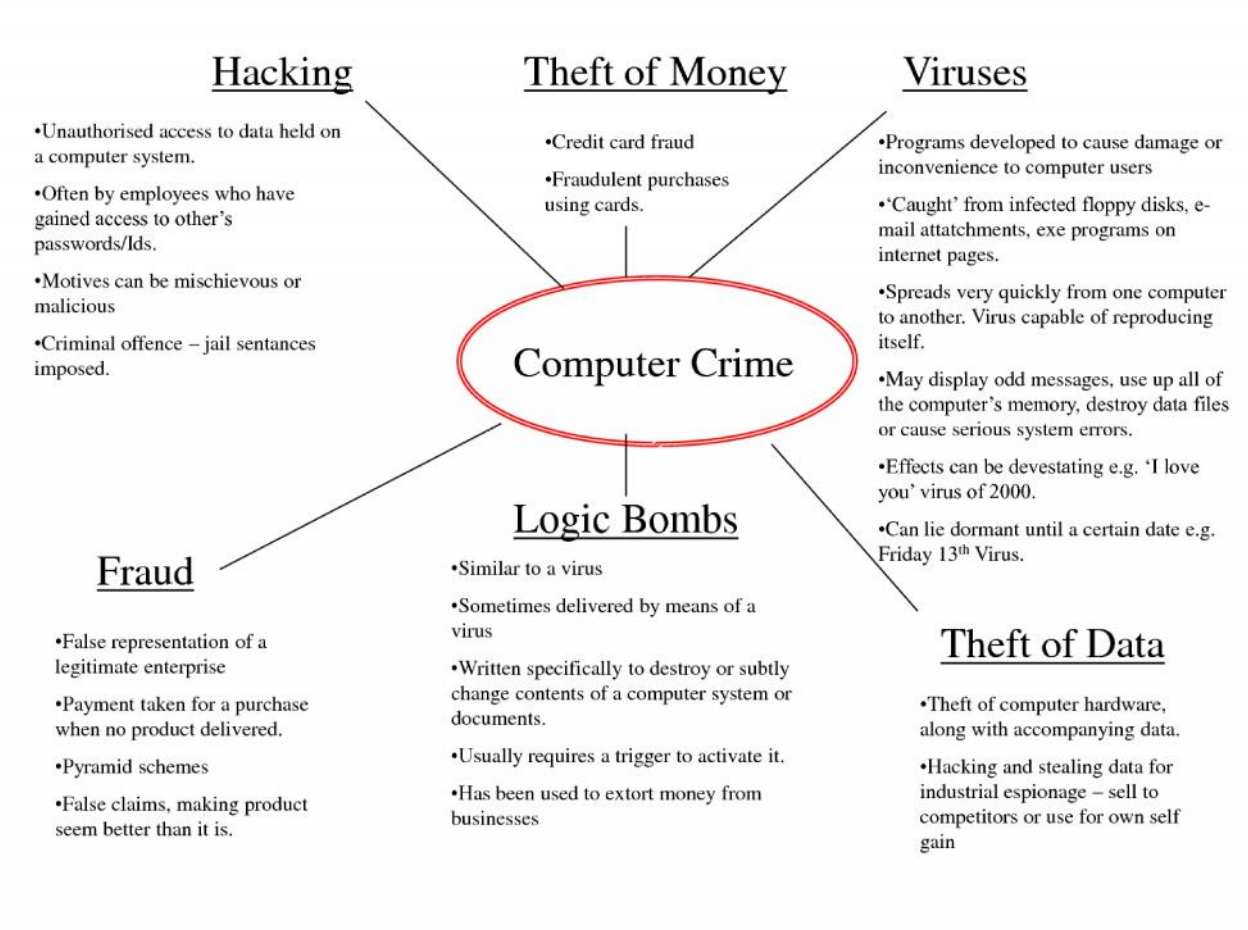
Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

What are the types of cyber crimes?

Computer crime encompasses a broad range of activities. It may be divided into two categories:

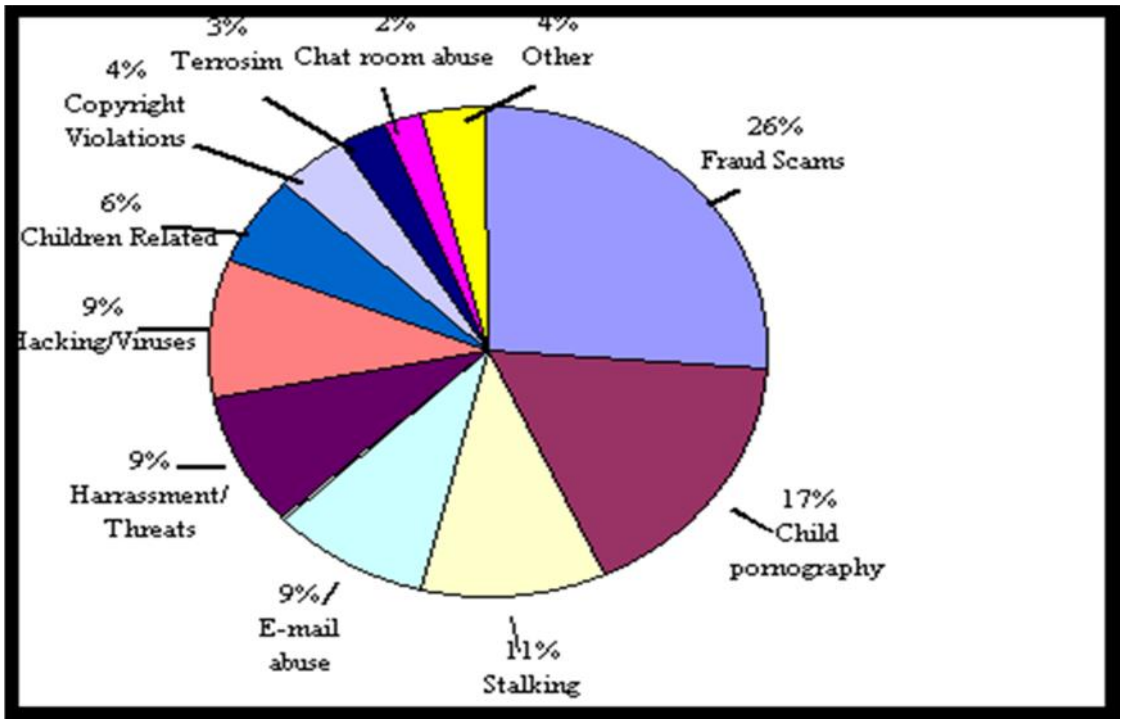




Threats

Various threats associated with cyber crime are -

- **Drug trafficking**- Drug traffickers are increasingly taking advantage of the Internet according to cyber authorities and personnel to sell their illegal substances through encrypted e mail and other Internet Technology. Some drug traffickers arrange deals at cyber cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.



- **Cyber terrorism** -Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal official that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them. Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources. As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyber terrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

- **Cyber extortion-** is a form of cyber terrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than

20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.

- **Hacking:** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

- **Theft:** This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

- **Cyber Stalking:** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

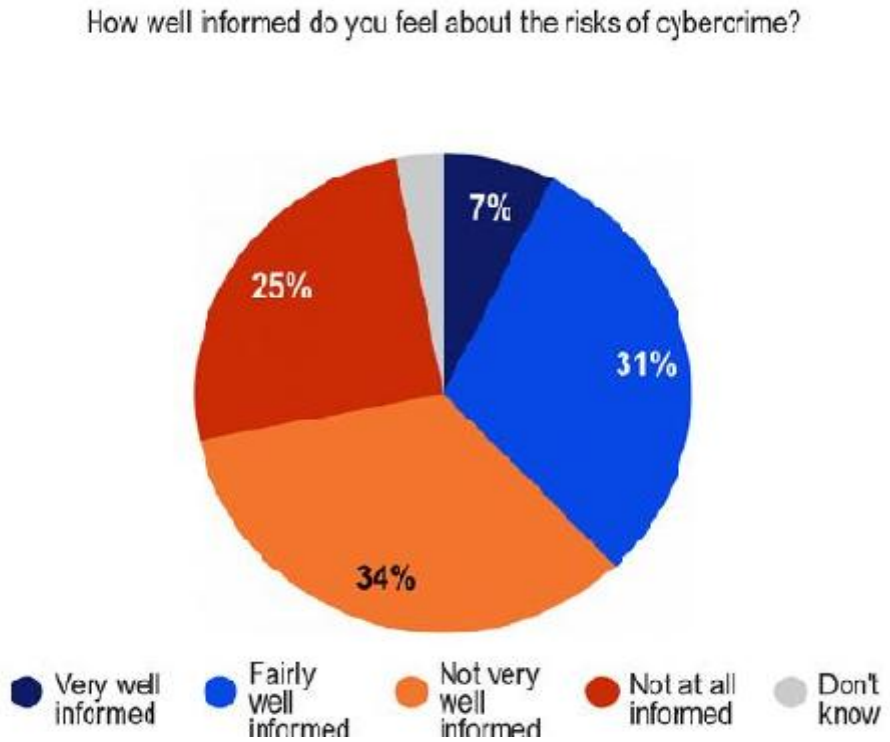
- **Identity Theft:** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

- **Malicious Software:** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

- **<u>Child soliciting and Abuse</u>:** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

Can cyber crimes be prevented?

It has to be mentioned that not many people are aware about cyber crime and its related issues. the pie graph shown below gives us a rough idea as to how many people are informed about cyber crimes and its related issues .



Cyber crimes can affect the society at three different levels they are –

- Individual
- Property
- Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

- **Individual:** This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

- **Property:** Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

- **Government:** Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

Hence to combat cyber crime one needs to increase awareness about this issue.

It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective.

- The best way to go about is using the solutions provided by Cross-Domain Solutions. When organizations use cross domain cyber security solutions, they can ensure that exchange of information adheres to security protocols. The solution allows organizations to use a unified system comprising of software and hardware that authenticates both manual and automatic

transfer and access of information when it takes places between different security classification levels. This allows seamless sharing and access of information within a specific security classification, but cannot be intercepted by or advertently revealed to user who is not part of the security classification. This helps to keep the network and the systems using the network safe.

- Cross Domain Solution offers a way to keep all information confidential by using safe and secure domains that cannot be tracked or accessed. This security solution can be used by commercial and governmental organization to ensure an impenetrable network while still making sure that users can get access to the required information easily. These measures may be able to reduce the cyber crimes.

SUDARSHANA SINHA
3RD YEAR, GEOGRAPHY (H)

DID YOU KNOW ???

Computers and the Internet offer great benefits to society. However, they also present opportunities for criminal activities such as fraud and identity theft. As an Internet user, it is important that you have a clear picture of what cybercrime actually is so that you can take steps to reduce your risk.

QUESTIONS

Q1. If you do not purchase goods or services on the Internet, you can't become a victim of cybercrime. **True/ False**

Q2. Purchasing goods or services on the Internet is safe, as long as you are connected to a Web site that supports secure transactions. **True/ False**

Q3. The Internet is so big that things like fraud or identity theft shouldn't really concern you; the probability you will be targeted is very small unless you use the Internet a lot. **True/ False**

Q4. Viruses, worms and other older forms of malicious software are nuisances created by reckless teenagers. Spyware is the main problem today and is funded by criminals. **True/ False**

Q5. Bots (short for "robot") are all over the Internet. Some are good, some are bad but they are here to stay. **True/ False**

Q6. You are protected against identity theft on the Internet if you have a firewall to keep out intruders, hackers and criminals. **True/ False**

Q7. There's little risk involved in letting other people use your computer - as long as they are family members. **True/ False**

Q8. Not all programs are at risk. For example, photographs can't contain harmful code. **True/ False**

Q9. People who don't use Microsoft Windows are safe. The bad guys take advantage of Windows users because it is easy and leave Linux and Macintosh users alone. **True/ False**

Q10. A legitimate company will not ask for personal information in an email message. Even though it may look convincing, messages that urgently request personal information are likely bogus. **True/ False**

ANSWERS

A1. **FALSE**

While secure connections are certainly an encouraging sign, it may only be indicating that the communications between you and the Web site are protected. It does not always mean that you are at the Web site you think you are! Online fraudsters have become increasingly sophisticated and sometimes leverage secure connections to lull the victim into a false sense of security because the padlock icon is illuminated in the browser. A secure connection to a fraudulent Web site still results in your data falling in the hands of the cybercriminal.

TIP: Practice safe online shopping. Know your sellers and use only secure sites.

A2. **FALSE**

Even people who do not shop or bank online can be affected by cybercrime. All it takes is one visit to a hostile website, or even a benign website with an infected advertisement, and a machine can be infected with a crime ware program such as a boot or Trojan horse.

TIP: Use secure transactions when transferring sensitive information and make sure you are dealing with a reputable company.

A3. **FALSE**

Automated boot programs are constantly scouring the Internet looking for fresh victims to infect. Even if you keep a low profile, the security of your computer will be tested by this relentless breed of crimeware. Moreover, the sheer volume of fraudulent "phishing" emails means that you are likely to receive a phony message sooner or later. While heavy Internet users may have more opportunities to become a victim, everyone using the Internet is exposed to the threat.

TIP: Read our Cybercrime stories to learn more about how real people are affected by online fraud.

A4. **FALSE**

While spyware is driven by a company`s desire to make money, so is the rest of crimeware, including bots, Trojan horses and even some worms. Malicious boot and Trojan horse authors are professional criminals rather than playful adolescents, creating their ill-intentioned programs to sell on the black market for a profit. They run promotions, offer trial versions of their programs, and provide customer support to the thieves who purchase their crimeware.

TIP: Check out our prevention tips to avoid becoming a victim of online fraud.

A5. **TRUE**

While the multi-purpose bots used in crimeware attacks are certainly malicious, bots are used across the Internet for performing many automated tasks such as assisting with shopping, managing Web sites and searching for news group articles of interest to the user. Bot software, both good and bad is often powerful, sophisticated, and easy to use; all reasons that bot programs, both helpful and harmful, will be with us for a long time.

TIP: Learn more about bots and how to protect yourself.

A6. **FALSE**

Firewall software is an excellent first step towards securing your computer, but it is only the first line of defense. In fact, software alone cannot completely protect you from online identity theft - today's attacks can be psychological in nature, luring the victim into providing confidential information rather than exploiting a software flaw.

TIP: Learn more about phishing and pharming, and how you can avoid these online scams.

A7. **FALSE**

Anyone can be attacked on the Internet. Cybercriminals use automated tools to send millions of fraudulent emails in the hopes of finding a small number of vulnerable victims. They don't care who provides the hole they need to infect a machine, be it a spouse or a child, anyone is capability of being duped into making a mistake. Cybercriminals work quickly - a moment of bad judgment is all that is needed to open Pandora's Box.

TIP: Choose strong passwords and keep them safe.

A8. **FALSE**

Many recent software problems involve attackers sending attack code embedded in image files, such as photographs, to victims. The attack takes place when the victim is surfing the Web or

reading an email and they encounter a Web page or message containing the contaminated photograph. When the photo is displayed, the attack code is triggered, infecting the victim's computer with crimeware.

TIP: Make sure to verify the authenticity of an attachment before you open it. More information on keeping your computer free of malware and unwanted software.

A9. **FALSE**

While Microsoft Windows users are certainly the most targeted population of Internet users, people using other operating systems and software are not immune to software flaws and fraud attacks. For example, the Firefox web browser had more confirmed vulnerabilities (25) than Internet Explorer (13) for the first half of 2005. This demonstrates that computer users cannot expect to eliminate their risk of attack online simply by choosing different software. Many of today's attacks such as phishing work independent of whatever software package you happen to be using.

TIP: Know what to do if you are targeted by cybercriminals

A10. **TRUE**

Even before phishing messages became as prevalent as they are today, it was uncommon practice to request confidential information using email.

TIP: Never send your personal information (credit card numbers, passwords, etc.) in an email

NIDHI BAID

3RD YEAR, PSYCHOLOGY HONOURS

SNS, THE BREEDING GROUND OF CYBER-HARASSMENT

In the age of Facebook, Instagram, Snapchat and other social networking sites, the internet has become the most convenient tool for stalkers and harassers. Cyber-bullying is when a child/preteen/teen is threatened or harassed in any way by another child/preteen/teen, via the internet or electronic technology. If an adult is involved, it is called cyber-stalking or cyber-harassment. These activities are now considered as cybercrimes, though not as publicized as other cybercrimes such as piracy or identity theft.

Prior to February 2013, there were no laws to directly regulate cyber-stalking in India. There were laws focusing on financial crimes and piracy, however, nothing related to interpersonal criminal behavior. In 2013, Indian parliament made amendments to the Indian Penal Code, introducing cyber-stalking as a criminal offence. A man committing the offence of stalking a woman would now be liable for imprisonment up to three years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to five years and with fine.

However, hardly anyone is aware of these laws. A lot of people get harassing messages on social media sites, repeated random phone calls and messages from unknown numbers at late hours, but hardly anybody reports this. I myself have had to change my phone number on two occasions to escape continuous phone calls from various unknown number late at night and random indecent messages. Even if threatened to be reported to the police, they just laugh and simply continue the harassment. Various people receive indecent messages on Facebook from random strangers, indecent photographs through direct message on Intagram, etc. People often get their Facebook accounts hacked into and those accounts are often used to carry out such activities. These things have become fairly common. In fact, they have become so common that we have simply learnt to ignore them. Girls are twice as likely to be the target of such harassing activities, compared to boys. Till date if these cybercrimes are only committed to annoy the victims and does not result in serious offences like severe defamation, sexual crimes, identity theft, or grave crimes like terrorism, it is treated as a bailable offence.

To quote some statistics, children in India reported the third highest online bullying rate after China and Singapore, among 25 countries surveyed under a recently commissioned project by Microsoft Corporation. The survey indicated that in India 77% of children reported being bullied online and/or offline. A survey conducted by antivirus company McAfee among 500 children and 496 parents in 10 cities of India indicated that 12% of children admitted to being victims of cyber -bullying or online intimidation; 20% of parents are unaware of the existence of cyber-bullying and 42% of children are not open to their parents about their online activities. It is a national epidemic and a global issue that must be fought against, with the same amount of vigor the government uses to fight against violent offence.

As a victim, an easy way to tackle cyber-harassment is to first recognize the situation for what it is, a crime. Then a copy should be made of the message/photo/video via a screenshot, save all communication for evidence, and the website operators should be contacted and informed that you are filing a case with the local police department and then file a report to the police department. The website operators should also be asked to take down the offending content from the website as well. We need to be proactive when it comes to online safety and privacy. Do not share personal information on any public space online. While these steps are not fool-proof and does not guarantee protection from cyber-harassment, it does help to avoid it to a large extent.

Cyber-stalking, cyber-harassing and cyber-bullying are just as bad a crime as piracy or identity theft, and it must be treated as such. It should not be ignored and it most definitely should not be tolerated. If one is a victim of these types of cybercrimes, one must report it and procure police protection against it. Once the people who commit these crimes realize that they cannot get away with committing it just because they are doing it online, or have the protection of an anonymous identity, they may stop. Or we may hope that at least they think twice before committing the crime anyway, because let’s face it, people have no shame.

VAISHALI MITRA
3RD YEAR, PSYCHOLOGY (H)

ACKNOWLEDGEMENTS

EDITOR

NIDHI BAID, 3RD YR
PSYCHOLOGY HONOURS

SUDARSHANA SINHA, 3RD YR
GEOGRAPHY HONOURS

NAOMI CHATTERJEE, 2ND YR
PSYCHOLOGY HONOURS

COVER DESIGNED BY

NEHA IMRAN, 3RD YR
EHGLISH HONOURS