The Study of Cyber Crime in India: Impact on Society and its Prevention

Saroj Kumari
(Assistant Professor, Forte Institute of Technology, India)

Abstract

The web could be a international system of interconnected pc networks that use the quality Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. the netcarries an enormous vary of knowledge resources and services, like the inter-linked hypertext documents of the globe Wide internet (WWW) and also the infrastructure to support electronic message. Through web and web, anybody will access info at any time and any wherever however the info that is available on-line will be targeted by person in a very method of hacking, pishing, etc. to damage {the computer|the pc} and data hold on in computer or available on-line. this kind of happening is termed cyber crime. Cyber crime continuously involves a point of infringement on the privacy of others or injury to computer-based property like files, web content or software system. This paper is totally targeted on cyber crime issue, trends and drawback faced by Indian users and the way cyber crimes will be reduced by formulating effective cyber crime laws in India. The paper additionally includes Indian cybercrime Statistics, cyber crime cells everywhere India and lots of additional latest news. National level agencies willdevelop security tips and policy to stop and safeguard of web users from cyber crimes.

Keywords: *Internet, WWW, Cyber world, Cyber crime, Hacking, Cyber laws, Indian cybercrime Statistics, Cyber cells in India*

INTRODUCTION

Our life is becoming more digitalized with the rapid technological developments. Be it business, education, shopping or banking transactions, almost everything is on the cyber space today. Cybercrime is evolving at an astounding pace, following the same dynamics as the inevitable penetration of computer technology and communication into all walks of life. In information technology data protection or information security is one of the great challenges for the world. It is one of the serious issues in information industry. Internet is one of the important and very fast growing commodities for development of business as well as in different private and government organizations. It is being used as the largest communication and information exchange medium now. At the same time Internet is becoming an instrument of numerous types of cyber crimes. It is being used to stealand manipulate the information of users. Important data is being stolen and personal as well as organizational threats are being imposed upon the users which are using Internet. Sensitive information, secret credentials and

even the bank account details are being stolen these days with the use of Internet. Cyber security is becoming a serious issue for the complete world with intruders attacking people or organizations with the motive of getting access to their restricted content. Cyber attackers are enjoying a renaissance with the increasing availability of bandwidth, connected devices, and affordable attack tools that allow them to launch evermore complex and potent attacks against a cyber security practitioner's (CSP's) residential subscribers and businesses. The threat to cyber security is growing at vast rate. Cyber criminals are becoming more sophisticated and are now targeting consumers as well as public and private organizations. Cyber crimes are rising due to the lack of cyber security. Many researchers have reported1-3 the issues related to cyber security in past.

These days' computer and internet become very Necessary and useful for our daily life. Today the internet is the great mediator of our lives. In present days people can get information, store information and share information through the internet. Back 20's years later there was approx.100000 people uses internet but now around 3,405,518,376 people are surf the net around the globe. The growing fastest world of internet is known as cyber world. Today cyber world are fastest moving and high technology world. Asian countries are most uses of internet in the world.

CYBER CRIME

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is additionally a crime to sell or elicit the higher than info on-line. Cyber crime could be a term for any criminal activity that uses a laptop as its primary means that of commission and thievery. The U.S. Department of Justice expands the definition of cyber crime to incorporate any illegal activity that uses a pc for the storage of proof. The growing list of cyber crimes includes crimes that are created doable by computers, like network intrusions and also the dissemination of pc viruses, additionally as computer-based variations of existing crimes, like fraud, stalking, bullying and coercion that became as major drawback to individuals and nations.Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolentprograms. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

What are Cyber Crimes?

Cyber Crimes in India are registered under three broad heads, the IT Act, the Indian Penal Code (IPC) and other State Level Legislations (SLL). The cases registered under the IT Act include

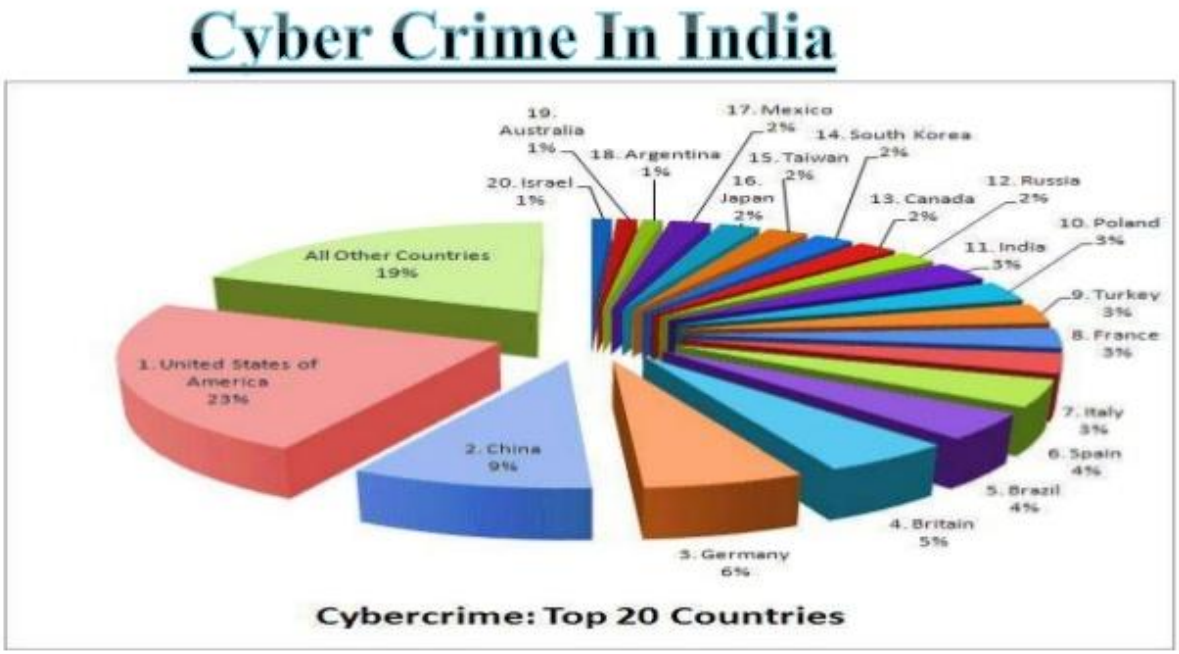
- Tampering computer source documents (Section 65 IT Act)
- Loss /damage to computer resource/utility (Section 66 (1) IT Act)
- Hacking (Section 66 (2) IT Act)
- Obscene publication/transmission in electronic form (Section 67 IT Act)
- Failure of compliance/orders of Certifying Authority (Section 68 I T Act)
- Failure to assist in decrypting the information intercepted by Govt Agency (Section 69 IT Act)
- Un-authorised access/attempt to access to protected computer system (Section 70 IT Act)

- Obtaining licence or Digital Signature Certificate by misrepresentation / suppression of fact (Section 71 IT Act)
- Publishing false Digital Signature Certificate (Section 73 IT Act)
- Fraud Digital Signature Certificate (Section 74 IT Act)
- Breach of confidentiality/privacy (Section 72 IT Act)
- Others

On the other hand, cases are also registered under the IPC and those include

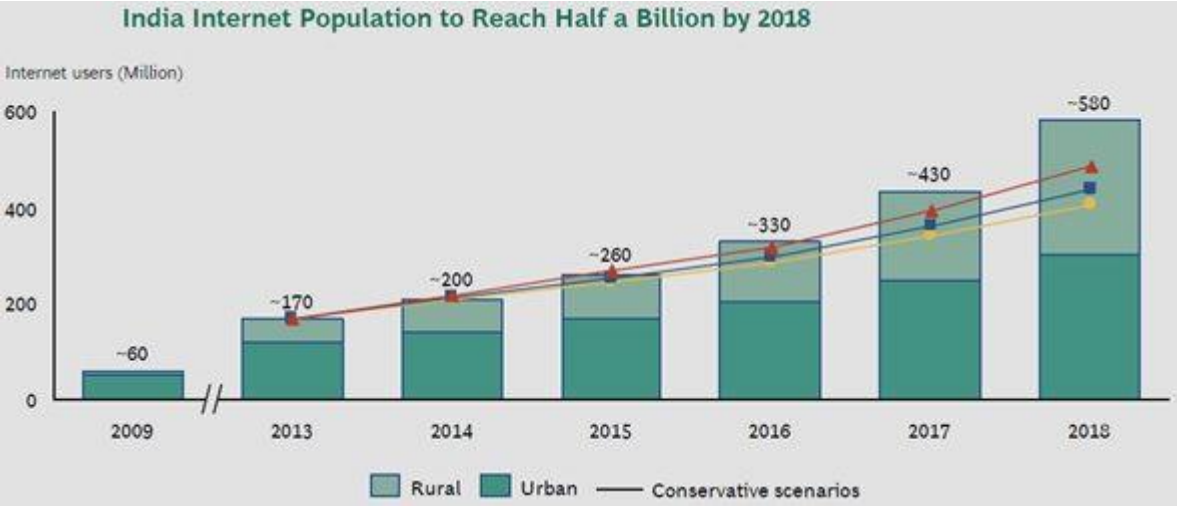
- Offences by/against Public Servant (Section 167, 172, 173, 175 IPC)
- False electronic evidence (Section 193 IPC)
- Destruction of electronic evidence (Section 204, 477 IPC)
- Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476, 477A IPC)
- Criminal Breach of Trust (Section 405, 406, 408, 409 IPC)
- Counterfeiting Property Mark (Section 482, 183, 483, 484, 485 IPC)
- Tampering (Section 489 IPC)
- Counterfeiting Currency / Stamps (Section 489A to 489E IPC)

\



https://www.google.com/search?q=latest+data+of+cyber+crime+in+india&tbm=isch&tbs=rimg:Cfp8fiGq4JMfIjgCD1_18T0InRfpnz-LuVnNWOus5f2LxdHT1vZ2NnyCb6Xdz9x-_1Aua7KB3msztitrx43-Bm8QbzXSoSCQIPX_1xPQidFEdmnSoz2iR_1kKhIJ-mfP4u5Wc1YR7BgKmYHDiYcqEgk66zl_1YvF0dBEx1p4FMogXNioSCfW9nY2fIJvpEfxpFQ2iD0VyKhIJd3P3H78C5rsRqJJBLh0cZSIqEgkoHeazO2K2vBFrFhe33ii06CoSCXjf4Gbx

BvNdETR8FH2IHMJW&tbo=u&sa=X&ved=2ahUKEwjd3N3rrZDgAhUZb30KHXaQBAkQ9C96BAgBEBg&biw=1366&bih=608&dpr=1#imgdii=XauA3XlijGYpcM:&imgrc=KMjzlzrqLdPNZM:



Categories of crime

There are 3 major classes that cybercrime falls into: individual, property and government. the kinds of strategies used and issue levels vary depending on the class.

•**Property**: this can be almost like a real-life instance of a criminal lawlessly possessing an individual's bank or mastercard details. The hacker steals a person's bank details to achieve access to funds, create purchases on-line or run phishing scams to induce folks to provide away their data. they might additionally use a malicious code to achieve access to an online page with confidential information.
•**Individual**: This class of cybercrime involves one individual distributing malicious or illegal info on-line. this could include cyberstalking, distributing creative activity and trafficking.
•**Government**: this can be the smallest amount common cybercrime, however is that the most serious offense. against the law against the govt is additionally called cyber terrorist act. Government crime includes hacking government websites, military websites or distributing information. These criminals are sometimes terrorists or enemy governments of different nations.

Types of cybercrime

DdoS Attacks

These are used to build an internet service unprocurable and take the network down by overwhelming the location with traffic from a range of sources. massive networks of infected devices called Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

Botnets

Botnets are networks from compromised computers that are controlled outwardly by remote hackers. The remote hackers then send spam or attack different computers through these botnets. Botnets may also be accustomed act as malware and perform malicious tasks.

Identity stealing

This cybercrime happens when a criminal gains access to a user's personal info to steal funds, access hint, or participate in tax or insurance fraud. they will additionallyopen a phone/internet account in your name, use your name to arrange a criminal activity and claim government advantages in your name. they'll do that by looking foruser's passwords through hacking, retrieving personal info from social media, or sending phishing emails.

Cyberstalking

This kind of crime involves on-line harassment wherever the user is subjected to a overplus of on-line messages and emails. usually cyberstalkers use social media, websites and search engines to intimidate a user and instill worry. Usually, the cyberstalker is aware of their victim and makes the person feel afraid or involved for his or her safety.

Social Engineering

Social engineering involves criminals creating direct contact with you always by phone or email. they require to realize your confidence and frequently create as a clientservice agent therefore you'll provide the required info required. this can be usually a countersign, the corporate you're employed for, or bank info. Cybercriminals canknow what they'll concerning you on the web and so try to add you as a friend on social accounts. Once they gain access to Associate in Nursing account, they'll sell your info or secure accounts in your name.

PUPs

PUPS or doubtless Unwanted Programs are less threatening than alternative cybercrimes, however are a kind of malware. They uninstall necessary code in your system as well as search engines and pre-downloaded apps. they'll embrace spyware or adware, therefore it's a decent plan to put in Associate in Nursing antivirus code to avoid the malicious transfer.

Phishing

This type of attack involves hackers causing malicious email attachments or URLs to users to realize access to their accounts or pc. Cybercriminals have become felt and lots of of those emails don't seem to be flagged as spam. Users are tricked into emails claiming they have to alter their countersign or update their request info, giving criminals access.

Prohibited/Illegal Content

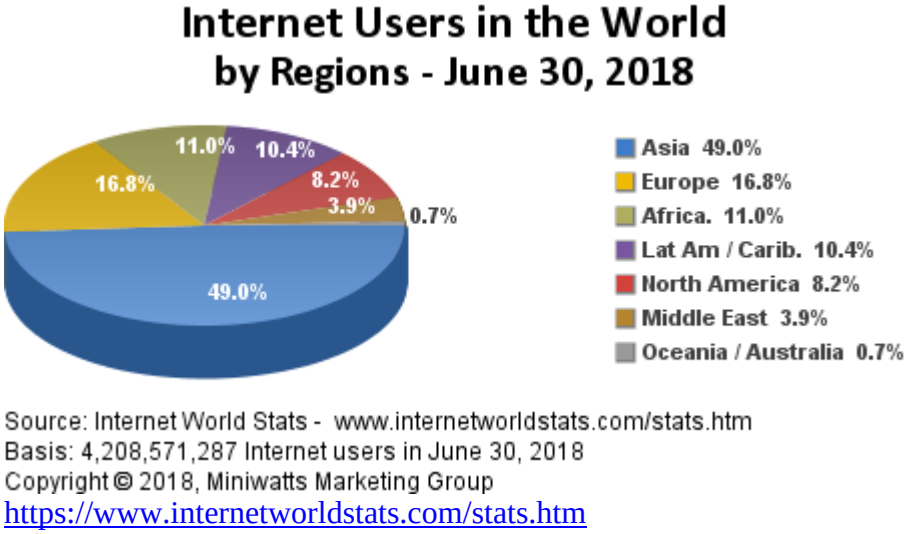
This crime involves criminals sharing and distributing inappropriate content that may be thought-about extremely distressing and offensive. Offensive content willembrace, however isn't restricted to, sexuality between adults, videos with intense violent and videos of criminal activity. black content includes materials advocating terrorism-related acts and kid exploitation material. this sort of content exists each on the everyday web and on the dark internet, Associate in Nursing anonymous network.

Online Scams

These are typically within the style of ads or spam emails that embrace guarantees of rewards or offers of surreal amounts of cash. on-line scams embrace engagingoffers that are "too sensible to be true" and once clicked on will cause malware to interfere and compromise info.

Exploit Kits

Exploit kits want a vulnerability (bug within the code of a software) so as to realize management of a user's pc. they're readymade tools criminals can purchase on-line and use against anyone with a pc. The exploit kits are upgraded frequently kind of like traditional code and are on the market on dark internet hacking forums.

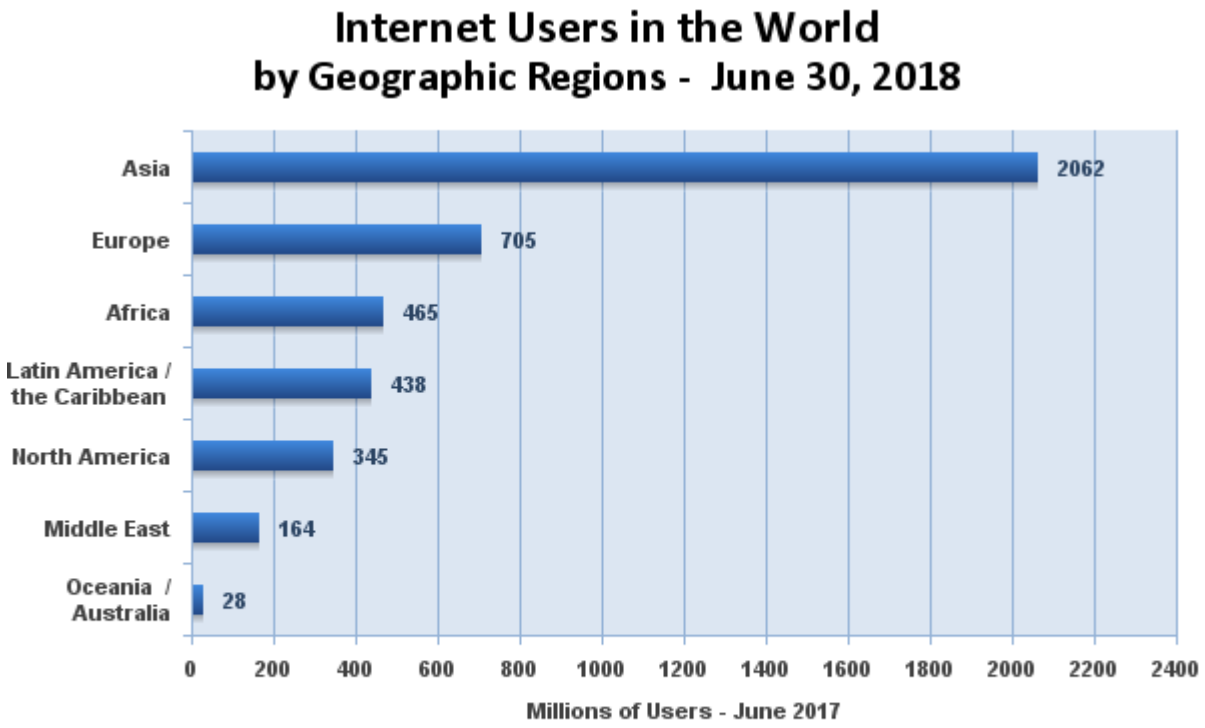


Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,208,571,287 Internet users in June 30, 2018
Copyright © 2018, Miniwatts Marketing Group
https://www.internetworldstats.com/stats.htm

WORLD INTERNET USAGE AND POPULATION STATISTICS
JUNE 30, 2018 – Update

World Regions	Population (2018 Est.)	Population % of World	Internet Users 30 June 2018	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	464,923,169	36.1 %	10,199 %	11.0 %
Asia	4,207,588,157	55.1 %	2,062,197,366	49.0 %	1,704 %	49.0 %
Europe	827,650,849	10.8 %	705,064,923	85.2 %	570 %	16.8 %
Latin America / Caribbean	652,047,996	8.5 %	438,248,446	67.2 %	2,325 %	10.4 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,894 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.2 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,208,571,287	55.1 %	1,066 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics estimates in June 30, 2018. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations Population Division. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide. (6) The information from this website may be cited, giving the due credit and placing a link back to www.internetworldstats.com. Copyright © 2018, Miniwatts Marketing Group. All rights reserved worldwide.



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,208,571,287 Internet users estimated in June 30, 2018
Copyright © 2018, Miniwatts Marketing Group

ASIA INTERNET USE, POPULATION DATA AND FACEBOOK STATISTICS - JUNE 30, 2018						
ASIA	Population (2018 Est.)	Internet Users, (Year 2000)	Internet Users 30-June-2018	Penetration (% Population)	Users % Asia	Facebook 31-Dec-2017
Afganistan	36,373,176	1,000	6,003,183	16.5 %	0.3 %	3,200,000
Armenia	2,934,152	30,000	2,126,716	72.5 %	0.1 %	990,000
Azerbaijan	9,923,914	12,000	7,999,431	80.6 %	0.4 %	1,800,000
Bangladesh	166,368,149	100,000	88,687,000	53.3 %	4.3 %	28,000,000
Bhutan	817,054	500	370,423	45.3 %	0.0 %	350,000
Brunei Darussalam	434,076	30,000	410,836	94.6 %	0.0 %	350,000
Cambodia	16,245,729	6,000	8,005,551	49.3 %	0.4 %	6,300,000
China *	1,415,045,928	22,500,000	802,000,000	56.7 %	38.9 %	1,800,000
Georgia	3,907,131	20,000	2,658,311	68.0 %	0.1 %	2,100,000
Hong Kong *	7,428,887	2,283,000	6,461,894	87.0 %	0.3 %	5,200,000
India	1,354,051,854	5,000,000	462,124,989	34.1 %	22.4 %	251,000,000
Indonesia	266,794,980	2,000,000	143,260,000	53.7 %	7.1 %	130,000,000
Japan	127,185,332	47,080,000	118,626,672	93.3 %	5.8 %	71,000,000
Kazakhstan	18,403,860	70,000	14,063,513	76.4 %	0.7 %	2,500,000

Korea, North	25,610,672	--	20,000	0.0 %	0.0 %	14,000
Korea, South	51,164,435	19,040,000	47,353,649	92.6 %	2.3 %	43,000,000
Kyrgystan	6,132,932	51,600	2,493,400	40.7 %	0.1 %	650,000
Laos	6,961,210	6,000	2,500,000	35.9 %	0.1 %	2,200,000
Macao *	632,418	60,000	512,352	81.0 %	0.0 %	380,000
Malaysia	32,042,458	3,700,000	25,084,255	78.3 %	1.2 %	22,000,000
Maldives	444,259	6,000	340,000	76.5 %	0.0 %	320,000
Mongolia	3,121,772	30,000	2,000,000	64.1 %	0.1 %	1,900,000
Myanmar	53,855,735	1,000	18,000,000	33.4 %	0.9 %	16,000,000
Nepal	29,624,035	50,000	16,190,000	54.7 %	0.8 %	8,700,000
Pakistan	200,813,818	133,900	44,608,065	22.2 %	2.2 %	32,000,000
Philippines	106,512,074	2,000,000	67,000,000	62.9 %	3.2 %	62,000,000
Singapore	5,791,901	1,200,000	4,839,204	83.6 %	0.2 %	4,300,000
Sri Lanka	20,950,041	121,500	6,710,160	32.0 %	0.3 %	5,500,000
Taiwan	23,694,089	6,260,000	20,821,364	87.9 %	1.0 %	18,000,000
Tajikistan	9,107,211	2,000	3,013,256	33.1 %	0.1 %	170,000
Thailand	69,183,173	2,300,000	57,000,000	82.4 %	2.8 %	46,000,000
Timor-Leste	1,324,094	0	410,000	31.0 %	0.0 %	390,000
Turkmenistan	5,851,466	2,000	1,049,915	17.9 %	0.1 %	20,000
Uzbekistan	32,364,996	7,500	15,453,227	47.7 %	0.7 %	800,000
Vietnam	96,491,146	200,000	64,000,000	66.3 %	3.1 %	50,000,000
TOTAL ASIA	4,207,588,157	114,304,000	2,062,197,366	49.0 %	100.0 %	818,934,000

NOTES: (1) The Asian Internet Statistics were updated in June 30, 2018. (2) The Facebook subscriber data were updated in Dec. 31, 2017. (3) CLICK on each country name to see detailed data for individual countries and regions. (4) The demographic (population) numbers are based mainly on data contained in United Nations Population Division and local official sources. (5) The usage numbers come from various sources, mainly from data published by Facebook , ITU , and other trustworthy sources. (6) For navigation help, definitions and methodology, please see the site surfing guide. (7) Data may be cited, giving due credit and establishing an active link back to Internet World Stats. (*) China figures do not include SAR Hong Kong, SAR Macao nor Taiwan, which are reported separately for statistical purposes.

IMPACTS OF CYBER CRIME:

The impacts of a single, successful cyber attack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and government is estimated to be billions of dollars a year. Criminals take advantage of technology in many different ways. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them

to ply their trade while hiding behind a shield of digital anonymity.

SECURITY COSTS: Cyber criminals also focus their attacks on businesses, both large and small. Hackers may attempt to take over company servers to steal information or use the machines for their own purposes, requiring companies to hire staff and update software to keep intruders out. According to EWeek, a survey of large companies found an average expenditure of $8.9 million per year on cyber security, with 100 per cent of firms surveyed reporting at least one malware incident in the preceding 12 months and 71 per cent reporting the hijacking of company computers by outsiders.

MONETARY LOSSES: The overall monetary losses from cyber crime can be immense. According to a 2012 report by Symantec, more than 1.5 million people fall victim to some sort of cyber crime every day, ranging from simple password theft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cyber crime worldwide every year. As consumers get wise to traditional avenues of attack, cyber criminals have developed new techniques involving mobile devices and social networks to keep their illicit gains flowing.

PIRACY: The cyber crime of piracy has had major effects on entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year. In response, copyright holders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allow copyright holders to target file sharers and sue them for large sums of money to counteract the financial damage of their activities online.

SOCIAL IMPACTS: Cyber criminals take full advantage of anonymity, secrecy, and interconnectedness provided by the Internet, therefore, attacking the very foundations of our modern information society. Cyber crime can involve botnets, computer viruses, cyber bullying, cyber stalking, cyber terrorism, cyber pornography, denial of service attacks, hacktivism, identity theft, malware, and spam. Law enforcement officials have struggled to keep pace with cyber criminals, who cost the global economy billions annually. Police are attempting to use the same tools cyber criminals use to perpetrate crimes in an effort to prevent those crimes and bring the guilty parties to justice. This article begins by defining cyber crime and then moves to a discussion of its economic and social impacts. It continues with detailed excursions into cyber bullying and cyber pornography, two especially representative examples of cyber crime, and concludes with a discussion of ways to curtail the spread of cyber crime.
Computer-related crimes date back to the origins of computing though the greater connectivity between computers through the Internet has brought the concept of cyber crime into public consciousness of our information society. "Billions of dollars in losses have already been discovered. Billions more have gone undetected. Trillions will be stolen, most without detection, by the emerging master criminal of the twenty-first century-the cyberspace offender" (Stephens, 1995, p. 24).

https://www.google.com/search?q=latest+data+of+cyber+crime+in+india&source=lnms&tbm=isch&sa=X&ved=0ahUKEwigh66xq5DgAhXSfCsKHR1ZDPEQ_AUIDygC&biw=1366&bih=608#imgdii=9b2djZ8gm-lt-M:&imgrc=-nx-Iargkx-8oM:

EMOTIONAL IMPACT OF CYBER CRIME:

A new study by Norton reveals the staggering prevalence of cyber crime. regarding sixty five per cent of net users globally, and seventy three per cent people internet surfers have fallen victim to cyber crimes, together with pc viruses, on-line mastercard fraud and fraud. because the most put-uponnations, America ranks third, once China (83 per cent) and Brazil and India (76 per cent). the primary study to look at the emotional impact of cyber crime shows that victims' strongest reactions ar feeling angry (58 per cent), irritated (51 per cent) and cheated (40 per cent), and in several cases, they blame themselves for being attacked. solely three per cent do not suppose it'll happen to them, associated nearly eighty per cent don't expect cyber criminals to be dropped at justice leading to an ironic reluctance to require action and a way of helplessness.

Despite emotional burden, the universal threat and incidents of cyber crime, folks still are not dynamic their behaviour - with solely 0.5 (51 per cent) of adults locution they'd amendment their behaviour if they became a victim. Even fewer than 0.5 (44 per cent) reportable the crime to the police. Nearly eighty per cent of cyber crimes ar calculable to originate in some variety of the underground market are attracting new actors with modest skills. Cyber crime is turning into a business chance receptive everyone driven by profit and private gain.

Cybercrime has created a serious threat to those that use the net, with many users' info stolen at intervals the past few years. it's additionally created a serious dent in several nations' economies. IBM president and chief operating officer union activity. The

diffusion of the model of fraud-as-service and therefore the diversification of the offerings of Ginni Rometty delineate crime as "the greatest threat to every profession.diversification of the offerings of Ginni Rometty delineate crime as "the greatest threat to every profession, every industry, every company in the world." Read below for shocking statistics on cybercrime's impact on our society to date.

- The global cost of cybercrime will reach **$6 trillion** by 2021.
- According to the Ponemon Institute's 2016 Cost of Data Breach Study, Global Analysis organizations that suffered at least one breach in 2016 lost an average of **$4 million**.
- **48% of data security breaches** are caused by acts of malicious intent.
- Cybersecurity Ventures expects ransomware costs will rise to **$11.5 billion in 2019**.
- Cybercrime will more than **triple the number** of unfilled cybersecurity jobs by 2021.

Prevention is usually higher than cure.

it's perpetually better to require sure precaution whereas in operation internet. A should build them his a part of cyber life. Saileshkumar Zarkar, technical adviser and network adviser to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for on-line security: Precaution, Prevention, Protection,

Cyber Crime prevention

1. **Use Strong Passwords**

   Use completely different user ID / password mixtures for various accounts and avoid writing them down. build the passwords additional difficult by combining letters, numbers, special characters (minimum ten characters in total) and alter them on a regular basis.

2. **Secure your computer**

   Activate your firewall

   Firewalls are the primary line of cyber defense; they block connections to unknown or fake sites and can exclude some kinds of viruses and hackers.

   Use anti-virus/malware software

   Prevent viruses from infecting your pc by putting in and frequently change anti-virus software.

   Block spyware attacks

   Prevent spyware from infiltrating your laptop by putting in and change anti-spyware package.

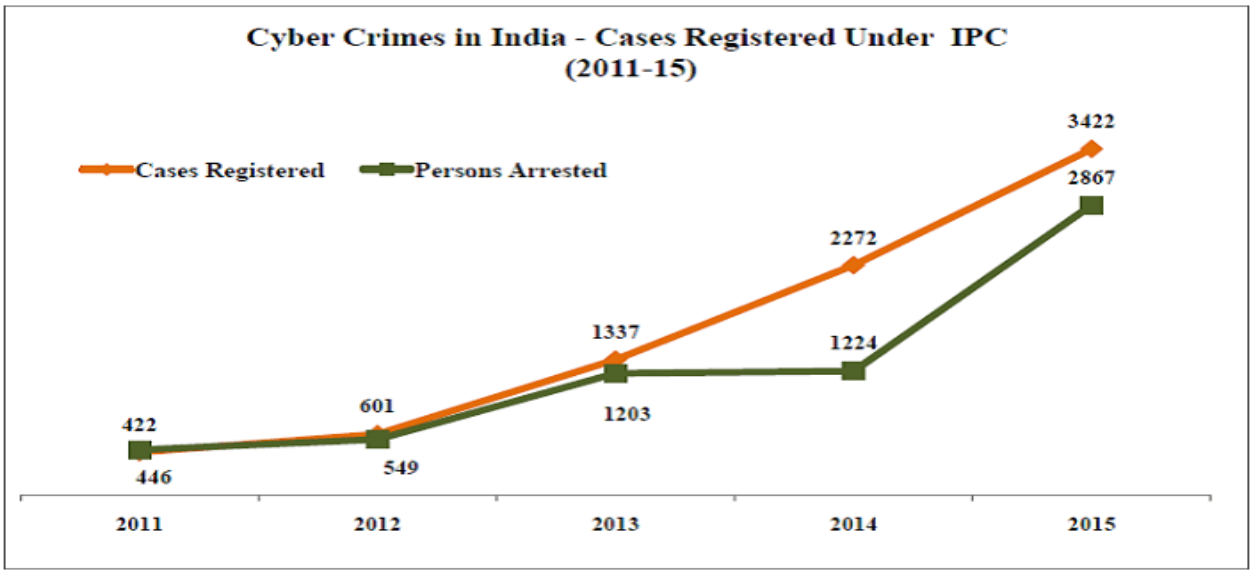
3. **Be Social-Media Savvy**

   Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) area unit set to non-public. Check your security settings. watch out what info you post on-line. Once it's on the web, it's there forever!

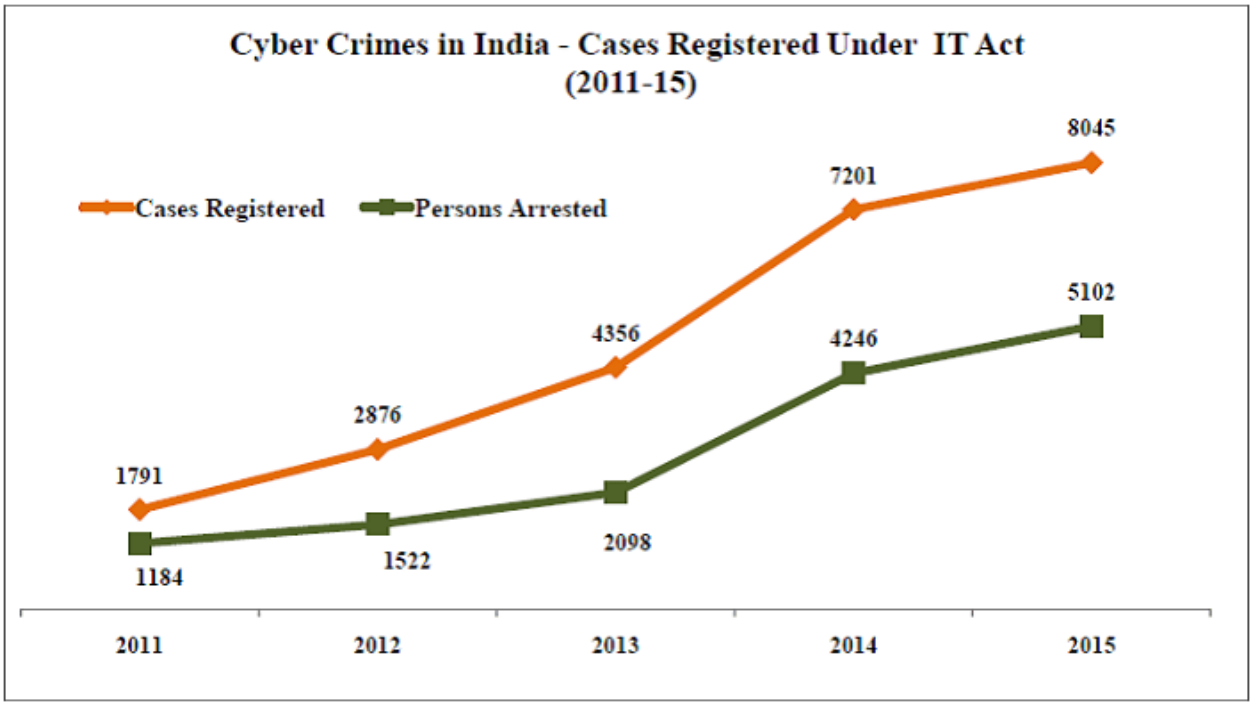
4. **Secure your Mobile Devices**

   Be aware that your mobile device is at risk of viruses and hackers. transfer applications from trustworthy sources.

5. **Install the most recent software package updates**
   Keep your applications and software package (e.g. Windows, Mac, Linux) current with the most recent system updates. activate automatic updates to forestall potential attacks on older package.
6. **shield your information**
   Use coding for your most sensitive files like tax returns or monetary records, build regular back-ups of all of your vital information, and store it in another location.
7. **Secure your wireless network**
   Wi-Fi (wireless) networks reception area unit at risk of intrusion if they're not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are vulnerable. Avoid conducting monetary or company transactions on these networks.
8. **Shield your e-identity**
   Be cautious once giving out personal info like your name, address, telephone number or monetary info on the web. certify that websites area unit secure (e.g. once creating on-line purchases) or that you've enabled privacy settings (e.g. once accessing/using social networking sites).
9. **Avoid being scammed**
   Always suppose before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the supply of the message. once doubtful, verify the supply. ne'er reply to emails that raise you to verify your info or ensure your user ID or word.
10. **Decision the proper person for facilitate**
    Don't panic! If you're a victim, if you encounter contraband net content (e.g. kid exploitation) or if you think a laptop crime, fraud or an advertisement scam, report this to your native police. If you would like facilitate with maintenance or package installation on your laptop, see your service supplier or a licensed laptop technician.



https://www.google.com/search?biw=1366&bih=608&tbm=isch&sa=1&ei=c-ZOXJ7ZBI7w9QOnsK7oCw&q=Statistics++of+cyber+crime+in+india+till+2018&oq=Statistics++of+cyber+crime+in+india+till+2018&gs_l=img.3...153457.164645..164840...3.0..0.351.5096.0j1j21j1.....0....1..gws-wiz-img.....0i7i30j0j0i30.jZsbKHogGsc#imgrc=5iVe3FyzihZvXM:



https://www.google.com/search?biw=1366&bih=608&tbm=isch&sa=1&ei=c-ZOXJ7ZBI7w9QOnsK7oCw&q=Statistics++of+cyber+crime+in+india+till+2018&oq=Statistics++of+cyber+crime+in+india+till+2018&gs_l=img.3...153457.164645..164840...3.0..0.351.5096.0j1j21j1.....0....1..gws-wiz-img.....0i7i30j0j0i30.jZsbKHogGsc#imgrc=lYPqLO9EWP_JFM:

What is the Government Doing?

The government says that use of social media has additionally emerged as a key tool for committing cyber crimes and attacks that have an effect on nation and society and is awake to increase in cyber crimes. it's taken numerousssteps within the type of awareness, training, legal framework, emergency response and implementation of best practices to stop incidence of such cyber crimes

In response to an issue within the Lok Sabha, the govt. mentioned that the subsequent measuresare being taken to tackle cyber crimes.

• The Ministry of Home Affairs has issued associate informatory to the State Governments and Union Territory Administrations on Cyber Crime. The State Governments are suggested to make adequate technical capability in handling cyber crime including technical infrastructure, cyber police stations and trained personnel for detection, registration, investigation and prosecution of cyber crimes.

• A major programme has been initiated on development of cyber forensics tools, fixing of infrastructure for investigation and coaching of the users, significantly police and judicial officers in use of this tool to gather and analyse the digital proof and gift them in Courts.

• Indian pc Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) arconcerned in providing basic and advanced coaching to enforcement Agencies, rhetorical labs and judiciary on the procedures and methodology of aggregation, analysing and presenting digital proof.

• Cyber forensics coaching workplace has been found out at coaching Academy of Central Bureau of Investigation (CBI) to impart basic and advanced coaching in Cyber Forensics and Investigation of Cyber Crimes to cops related to CBI. additionally, Government has found out cyber rhetorical coaching and investigation labs within

the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu for coaching of enforcement and Judiciary in these States.

• In collaboration with information Security Council of India (DSCI), NASSCOM, Cyber rhetorical Labs are found out at metropolis, Bengaluru, Pune and kolkata for awareness creation and coaching programmes on Cyber Crime investigation. National school of law, metropolis and NALSAR University of Law, Hyderabad are engaged in conducting many awareness and coaching programmes on Cyber Laws and Cyber crimes for judicial officers.

• The Indian pc Emergency Response Team (CERT-In) problems alerts and advisories concerning latest cyber threats and countermeasures on regular basis. CERT-In has revealed tips for securing the websites, that araccessible on its web site (www.cert-in.org.in). CERT-In additionally conducts regular coaching programme to form the system directors aware of secure hosting of the websites and mitigating cyber attacks.

• Government has determined to produce a centralized subject portal through Crime and Criminal pursuit Network and Systems(CCTNS) for registering on-line cyber crime complaints. The Ministry of Home Affairs has additionallyin-principle approved to line up an Indian Cyber Crime Coordination Centre (I4C) to fight against cyber crime within the country associated establish an open platform for victims to lift cybercrime complaints with the protocol for resolution like on-line crime coverage, to support and coordinate electronic investigations of law-breaking, assist the enforcement agencies in criminal investigation etc.

• The cyber area is being closely monitored by the govt. in respect of matters of radicalization tries. the govt. has additionally directed the intelligence agencies to spot potential recruits and keep them underneath surveillance.

Conclusion

Capacity of human mind is unfathomable. it's unfeasible to eliminate cyber crime from the cyber area. it's quite doable to ascertain them. History is that the witness that no legislation has succeeded in wholly eliminating crime from the world. the sole doable step is to form individuals attentive to their rights and duties (to report crime as a collective duty towards the society) and additional creating the appliance of the laws additional tight to examinecrime. beyond any doubt the Act could be a historical step within the cyber world. additional I all at once don'tdeny that there's a desire to bring changes within the info Technology Act to form it simpler to combat cyber crime. i'd conclude with a word of caution for the pro-legislation faculty that it ought to be unbroken in mind that the provisions of the cyber law aren't created therefore tight that it should retard the expansion of the trade and encourage be counter-productive.

Kamini Dashora, PhD, Principal, P.P. Patel school of Social Sciences, (Affiliated Sardar Patel University, Vidyanagar, Gujarat, India) ,Journal of different views within the Social Sciences (2011) Vol three, No 1, 240-259

References:

- *Tonge A. M., Kasture S. S., Chaudhari S. R., Cyber security: challenges for society-literature review, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, 12(2), 67-75 (2013).*

- *Dunn M., The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP), International Journal for Critical Infrastructure Protection, 1 (2/3), 58-68 (2005).*
- *Stoll C., The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage, New York: Pocket Books (1990).*
- *https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/*
- *https://www.internetworldstats.com/stats3.htm*
- *https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html*
- *https://www.internetworldstats.com/stats.htm*
- *Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India,New Delhi, India.*
- *Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.*
- *Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India*
- *Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.*
- *http://en.wikipedia.org/wiki/Computer_crime*
- *https://cybercrimelawyer.wordpress.com/category/66c-punishment-for-identity-theft/*
- *http://ncrb.nic.in/*
- *www.economictimes.indiatimes.com/*
- *http://in.norton.com/*
- *www.ncpc.org*
- *http://www.enotes.com/research-starters/social-impacts-cyber-crime*
- *https://cybercrimelawyer.wordpress.com/category/66c-punishment-for-identity-theft*