CYBER CRIMES IN INDIA: TRENDS AND PREVENTION

Ms. Riddhi Shah
Assistant Professor
Department of Information Technology
K.E.S. Shroff College of Arts and Commerce, Kandivali (west), Mumbai, India

Abstract: India is moving towards a digital era, and to be a part of digital India, Internet is needed. Internet is known as an interconnected network which allows to share any kind of information to anyone using any network connected device. In India, since last few years, usage of internet has been increased at very high rate. In Global ranking for internet users, India stands at second position worldwide. Every single person in India is having internet connected device Nowadays every essential tasks like shopping, paying of bills, paying of tax, transfer of money, communicating to a person globally, sharing of information, performing business and so on, are heavily dependent on internet. On one hand it is at ease of use on the other this leads to an increase of crimes using internet as a medium i.e., Cyber crimes. As internet usage increasing day by day, the vulnerabilities of their users are also increasing. This paper focuses on studying the growth trends of internet usage and the vulnerabilities faced by the users in India. Also studying the trends of reported cyber crimes in India under IT Act 2000 and Indian Penal Code (IPC) during year 2012-16 and it attempts to analyze the persistent as well as emergent types of cyber crimes occurred during years 2012-16 under IT Act 2000 and Indian Penal Code (IPC) respectively. Furthermore, this paper tries to study the emergent types of crime occurred in year 2017 along with the prevention measures taken by government of India and also suggests the best practices to avoid pit holes.

Index Terms: Internet Usage, Cyber crime, Growth trends, IT Act 2000, Indian Penal Code(IPC), Persistent, Emergent

I. INTRODUCTION

1.1 Cyber crime

Cyber crime is a crime which is performed using computer and internet to extract information from any other computer or device. National Crime Records Bureau (NCRB) defines cyber criminals perform cybercrimes to earn money, to become famous, to just have fun, to sexually exploit someone, to blackmail someone, for developing own business, for selling/purchasing illegal contents, to take a revenge of someone, or to do a prank with someone, and so on. The main advantage the criminals have, to perform their activities using internet is that they are not traceable easily. Since, internet is extended globally, it is very difficult for cyber officers or police to locate a cyber criminal because it can be performed anywhere around the world and tracing of this activity are spread through various locations which makes it a difficult task to perform. Therefore, it becomes even more difficult to caught hold of such criminals. In India, these type of crimes are reported and resolved under IT Act 2000 and Indian Penal Code. The details of the acts are as follows:

1.2 IT Act 2000

IT Act 2000 is an act of the Indian Parliament to deal with cyber crime and e-commerce. This is a law which applies to India as well as person outside India if the crime involves usage of computer with an internet. It provides a legal framework for e-governance which gives recognition to electronic record and digital signature. This act also describes the penalties for cyber criminals.

Table 1.2: Offences under IT Act 2000

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000
66A	Publishing offensive, false or threatening information	Imprisonment up to three years, with fine.
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person (Identity Theft)	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of Cyberterrorism	Imprisonment up to life
67	Publishing information which is obscene in electronic form	Imprisonment up to five years, or/and with fine up to ₹100,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to ₹100,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to three years, or/and with fine up to ₹200,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years and possible fine.
71	Misrepresentation	Imprisonment up to three years, or/and with fine up to ₹100,000
72	For Breach of confidentiality and privacy	imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
72A	For disclosure of information in breach of lawful contract	Punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

(Source: http://dot.gov.in/sites/default/files/itbill2000_0.pdf)

As per new amendment, section 66 is substituted by Act 10 of 2009 and thus, subsections 66(1) and 66(2) has been removed from the amendment and has been now merged in section 66 itself.

1.3 Indian Penal Code(IPC)

IPC covers all the criminal laws of India. Crimes recorded such as cheating, frauds, forgery, misappropriation, defamation using computer and sending threatening/defamatory messages by email, cyber frauds, credit/ debit card frauds, data and identity theft etc. are taken care under IPC. This act also describes the penalties for these cyber criminals.

Table 1.3: Cyber crime offences under IPC

Section	Offence	Penalty
193	Punishment for false evidence	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine
204	Destruction of document to prevent its production as evidence	Imprisonment of either description for a term which may extend to two years, or with fine, or with both.
379	Punishment for theft (Data Theft)	Imprisonment of either description for a term which may extend to three years, or with fine, or with both.
380	Theft in dwelling house, etc. (Data Theft)	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
381	Theft by clerk or servant of property in possession of master (Data Theft)	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
384	Punishment for extortion (Web Jacking)	Imprisonment of either description for a term which may extend to three years, or with fine, or with both.
406	Punishment for criminal breach of trust	Imprisonment of either description for a term which may extend to three years, or with fine, or with both.
408	Criminal breach of trust by clerk or servant	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
409	Criminal breach of trust by public servant, or by banker, merchant or agent	Imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.
420	Cheating and dishonestly inducing delivery of property	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
465	Punishment for forgery (electronic records)	Imprisonment of either description for a term which may extend to two years, or with fine, or with both.
466	Forgery of record of court or of public register, etc.	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
467	Forgery of valuable security, will, etc.	Imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.
468	Forgery for purpose of cheating	Imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
471	Using as genuine a forged document	punished in the same manner as if he had forged such document.
477A	Falsification of accounts	Imprisonment for life, or with imprisonment of either description for a term which

		may extend to seven years, and shall also be liable to fine.
489A	Counterfeiting currency-notes or bank-notes	Imprisonment for life or Imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.
489B	Using as genuine, forged or counterfeit currency-notes or bank-notes	Imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.
489C	Possession of forged or counterfeit currency-notes or banknotes	Imprisonment of either description for a term which may extend to seven years, or with fine, or with both.
489D	Making or possessing instruments or materials for forging or counterfeiting currency-notes or bank-notes	Imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine
489E	Making or possessing instruments or materials for forging or counterfeiting currency-notes or bank-notes	Imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine
500	Punishment for defamation (sending defamatory message by email)	Imprisonment for a term which may extend to two years, or with fine, or with both.
506	Punishment for criminal intimidation (sending threating message by email)	imprisonment of either description for a term which may extend to two years, or with fine, or with both;

(Source: https://www.ncib.in/pdf/indian-penal-code.pdf)

II. METHODS AND MATERIALS

2.1 Data Collection

Secondary data was used which was collected from the National Crime Records Bureau website to get the cyber crimes recorded during the Calendar Year 2012-2016 under IT Act 2000 and Indian Penal Code. Secondary data had also been collected from the 'Cyber Security' article published in NITI Aayog to study the emerging crimes recorded between the years Calendar Year 2012-2017. For capturing the ever emerging usage of internet in India, the secondary data had been collected from various websites such as internetlivestats, statista and iamai.

2.2 Data Analysis

A Trend analysis was performed to identify the population proportion of internet users across India to study the growth of internet usage in India during years 2012-2018.Also, Trend analysis of the number of cyber crimes recorded under IT Act 2000 and under IPC was performed. The cyber crimes under these acts are further categorised based on the observed occurrences of these crimes during the year 2012-16 into two categories viz. Persistent and Emergent. Persistent cyber crimes are those crimes which are repetitively recorded in consecutive year and Emergent cyber crimes are those crimes which are newly observed and non or less repetitive. 2D-Bar charts are used to analyse the newly emerging cyber crimes and also to express the distributions of recent cyber crimes for the year 2017.

Growth rate has been calculated using formula:

Growth rate (year wise)=

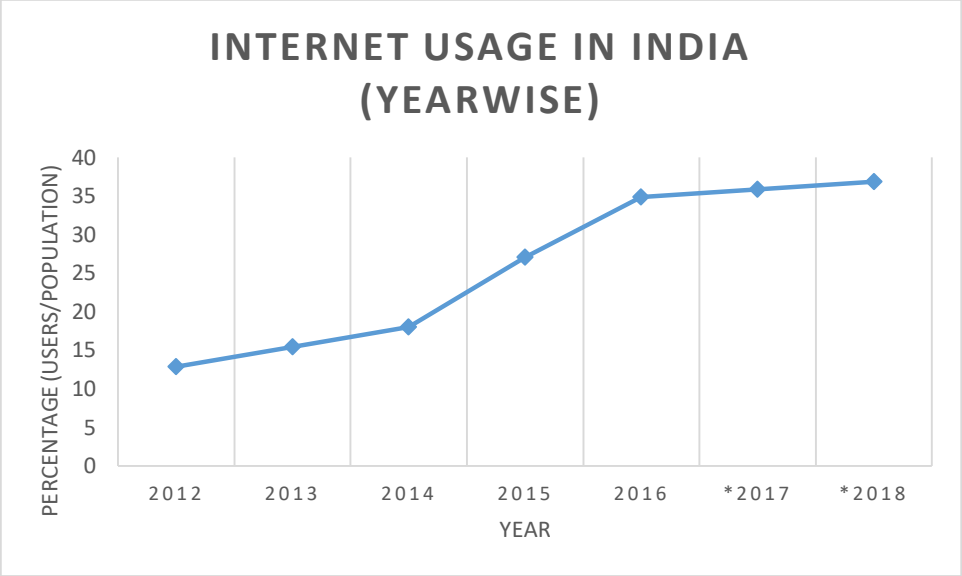
[(current year data- previous year data)/previous year data] *100

*2012 is considered as a starting year, thus growth rate has been calculated for year 2013 to 2016.

III. RESULTS AND DISCUSSION

3.1 Internet usage in India

Cyber crime is a crime which is performed using internet and any device mainly computer. To study the growth of internet usage in India, a percentage (users/population) was calculated between years 2012-2018.



*estimated users
(Source: IAMAI & Kantar IMRB I- CUBE 207, All India Users Estimates, October 2017)
Fig 3.1: Percentage (Users/Population) of Internet Usage in India between years 2012-18

Fig 3.1. Shows the trend in the usage of Internet in India between years 2012-18. Initially the growth of internet usage was consistent between years 2012-14 but it has been found because of rapid growth of buying a mobile phone along with cheaper rate and faster speed of internet subscription, free internet provision scheme by the network provider affected the rose of internet usage between years 2014-2016. In year 2017-18 it has been estimated to follow the consistency again. Table 3.1. Shows the growth percentage of internet usage in India.

Table 3.1: Growth Percentage of Internet Usage in India (year wise)

Year	**2012**	**2013**	**2014**	**2015**	**2016**	***2017**	***2018**
Percentage	12.88%	15.45%	18.01%	27.05%	34.89%	35.91%	36.91%

3.2 Cyber Crimes under IT Act 2000 - PERSISTENT

As the internet usage has been risen in India, the analysis of cyber crimes reported in India in those years has been studied.

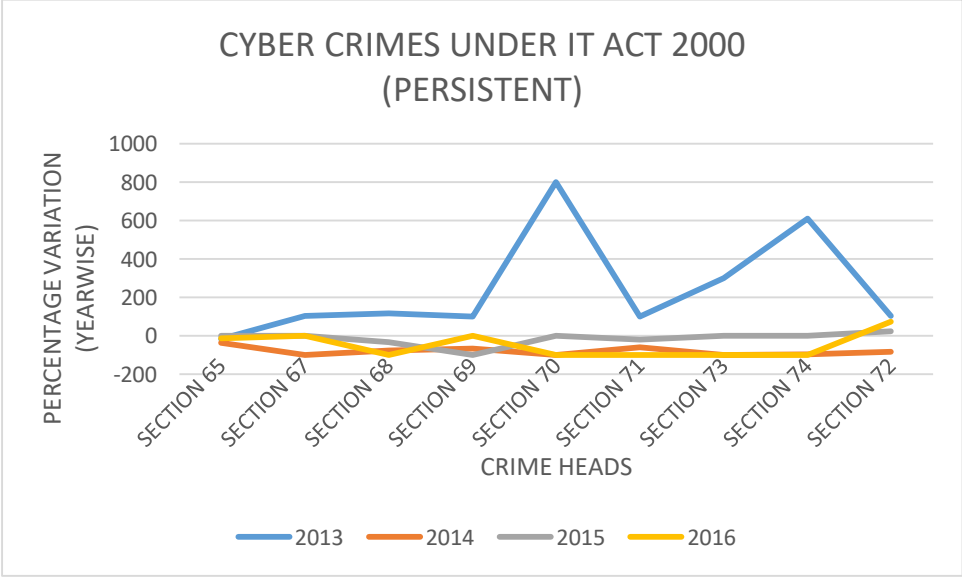


Fig 3.2: Persistent cyber crimes reported under IT Act 2000 between years 2012-16

Fig 3.2. Illustrates the year wise growth rate of persistent types of cyber crimes reported under IT Act 2000. Table 3.2. Shows the growth rate of persistent types of cyber crimes occurred between years 2012-16 under IT Act 2000. It has been found that the growth of crime has increased in 2013 and further reduced in year 2014 but under sections 70, 72 and 73 the cyber crimes has been again risen with very high growth rate in year 2015. Thus, It has been noticed that as the internet usage increases, the crimes using internet i.e., cyber crimes also increases.

Table 3.2: Growth rate of persistent cyber crimes under IT Act 2000 (year wise)

Crime Head / Year	Sec. 65	Sec. 67	Sec. 68	Sec. 69	Sec. 70	Sec. 71	Sec. 72	Sec. 73	Sec. 74
2012	-	-	-	-	-	-	-	-	-
2013	-14.90	104.24	116.67	100	800	100	102.17	300	610
2014	-35.03	-100	-76.92	-66.67	-100	-58.33	-82.79	-100	-95.77
2015	-1.12	0	-33.33	-100	#	-20	25	#	0
2016	-11.36	0	-100	0	-100	-100	75	-100	-100

(Source: National Crime Records Bureau website http://ncrb.gov.in/)
(negative % indicates decrease rate of crime, positive % indicates increase rate of crime)
# indicates the larger growth rate (i.e., near to infinity)

3.3 Cyber Crimes under IPC - PERSISTENT

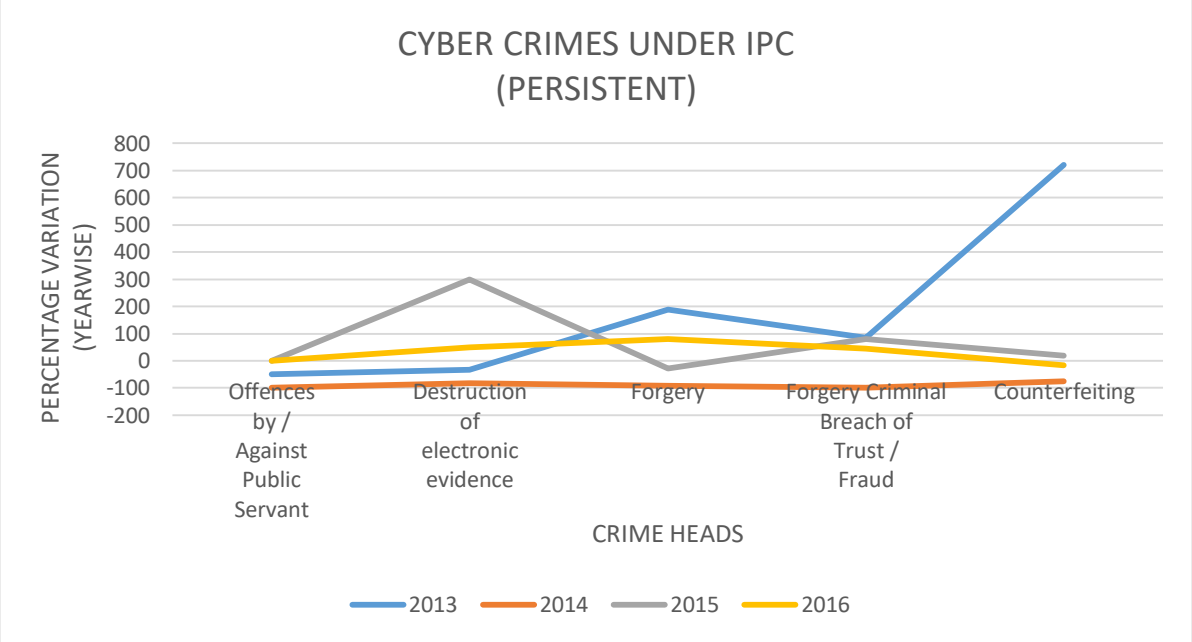


Fig 3.3: Persistent cyber crimes reported under Indian Penal Code(IPC) between years 2012-16

Fig 3.3. Illustrates the year wise growth rate of persistent types of cyber crimes reported under IPC. Table 3.3. Shows the growth rate of persistent types of cyber crimes occurred between years 2012-16 under IPC. It has been found that the growth of crime has increase in 2013 and further reduced in year 2014 and also has been analyzed that the growth rate of all persistent crimes under IPC has risen in year 2015 and 2016 which justifies the fact that as internet usage increases, crimes related to IPC also increases. Thus, It has been observed that cyber Crimes under IPC is occurring in each consecutive year.

Table 3.3: Growth rate of persistent cyber crimes under IPC (year wise)

Crime Head / Year	Offences by /Against Public Servant	Destruction Of electronic evidence	Forgery	Forgery Criminal Breach of Trust /Fraud	Counterfeiting
2012	-	-	-	-	-
2013	-50	-33.33	188.41	83.68	720
2014	-100	-83.33	-91.56	-98.07	-75.61
2015	0	300	-28.57	80	20
2016	0	50	80	44.44	-16.67

(Source: National Crime Records Bureau website http://ncrb.gov.in/)
(negative % indicates decrease rate of crime, positive % indicates increase rate of crime)

India is moving towards a digital era and that emerges multiple technology to be used for online transaction, online banking, online shopping, communication through social networking sites, online business through e-commerce to provide 24x7 customer service and satisfaction but this digitization also leads to the emergent of different new types of cyber crimes as well.

3.4 Cyber Crimes under IT Act 2000 – EMERGENT (2013)

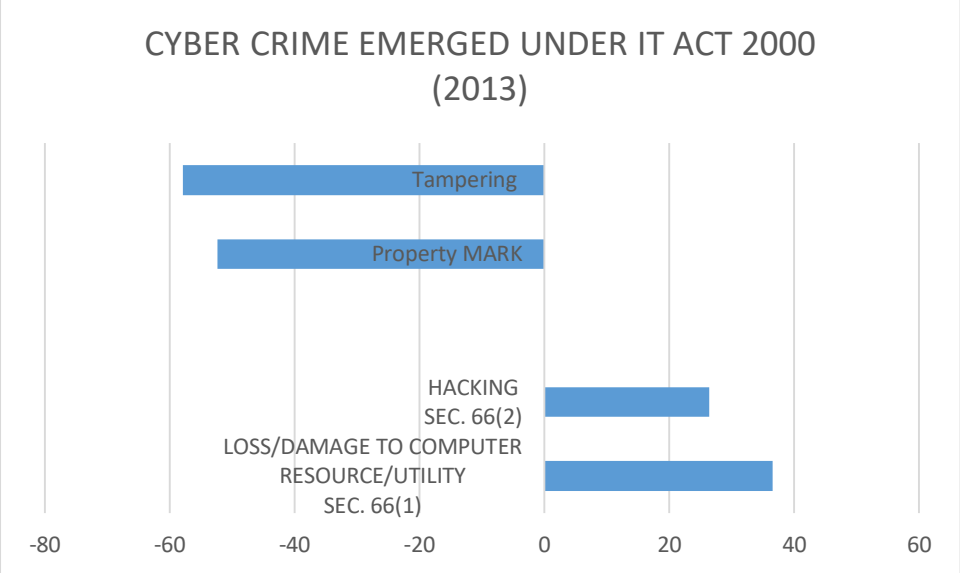


Fig 3.4: Emergent cyber crimes reported under IT Act 2000 in year2013

Fig 3.4. Represents the newly emerged cyber crimes reported under IT Act 2000 in year 2013. It has been noticed that crimes related to hacking, damage of computer resources has been emerged under section 66(1) and 66(2) of IT Act 2000 (Now section 66, as per new amendment). Also, Crimes related to tampering and property mark has been reduced by approximately 50% due to prevention measures taken by Indian Government in the same year. Table 3.4. Represents the growth rates of emergent cyber crimes under IT Act 2000 between year 2013.

Table 3.4: Growth rate of emergent cyber crimes under IT Act 2000 in year 2013

Crime Head / Year	loss/damage to computer resource/utility sec. 66(1)	hacking sec. 66(2)	Property mark	Tampering
2013	36.53	26.44	-52.38	-57.89

(Source: National Crime Records Bureau website http://ncrb.gov.in/)
(negative % indicates decrease rate of crime, positive % indicates increase rate of crime)

3.5 Cyber Crimes under IT Act 2000 – EMERGENT (2015)

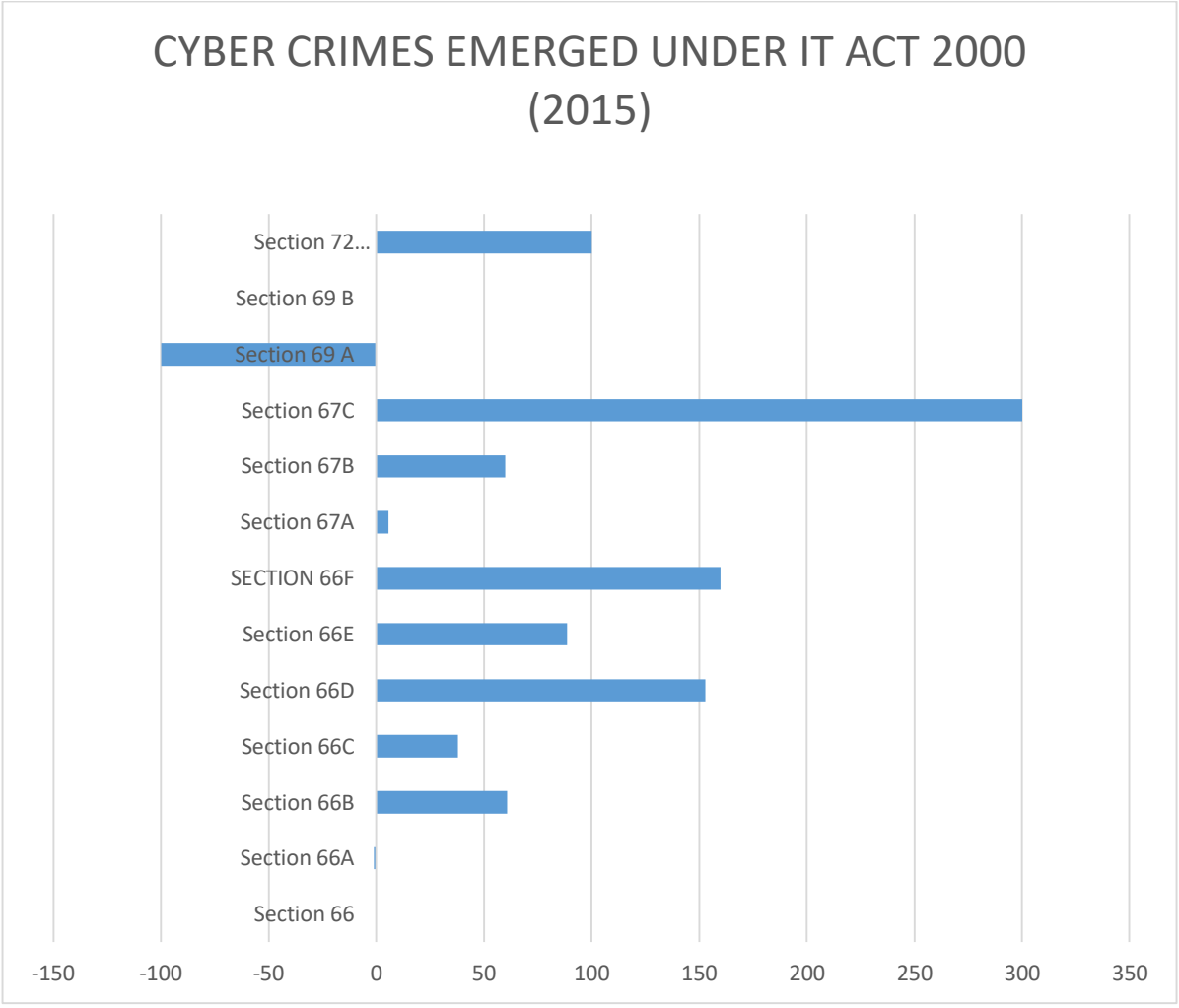


Fig 3.5: Emergent cyber crimes reported under IT Act 2000 in year 2015

After year 2013, it has been observed that there is no new cyber crime has been recorded in year 2014. But, As the usage of internet increased , few cyber crime has also been newly emerged in year 2015. Fig 3.5. Represents the emergent types of cyber crimes reported under IT Act 2000 in year 2015. It has been noticed that crimes under section 66,66A-66F,67A-67B has been emerged in year 2015. Table 3.5: Represents the growth rates of emergent cyber crimes under IT Act 2000 in year 2015.
It has been observed that the newly emerged crime is having the first instance of occurrence. Since, it does not have any previous history thus the growth rate of such crime is very large.

Table 3.5: Growth rate of emergent cyber crimes under IT Act 2000 between year 2015

Crime Head / Year	**Sec. 66**	**Sec. 66A**	**Sec. 66B**	**Sec. 66C**	**Sec. 66D**	**Sec. 66E**	**Sec. 66F**	**Sec. 67A**	**Sec. 67B**	**Sec. 67C**	**Sec. 69A**	**Sec. 69B**	**Sec. 72A**
2015	0	-0.90	60.97	37.88	153.0	88.70	160	5.74	60	300	-100	0	100

(Source: National Crime Records Bureau website http://ncrb.gov.in/)
(negative % indicates decrease rate of crime, positive % indicates increase rate of crime)

3.6 Cyber Crimes under IT Act 2000 – EMERGENT continued in 2016

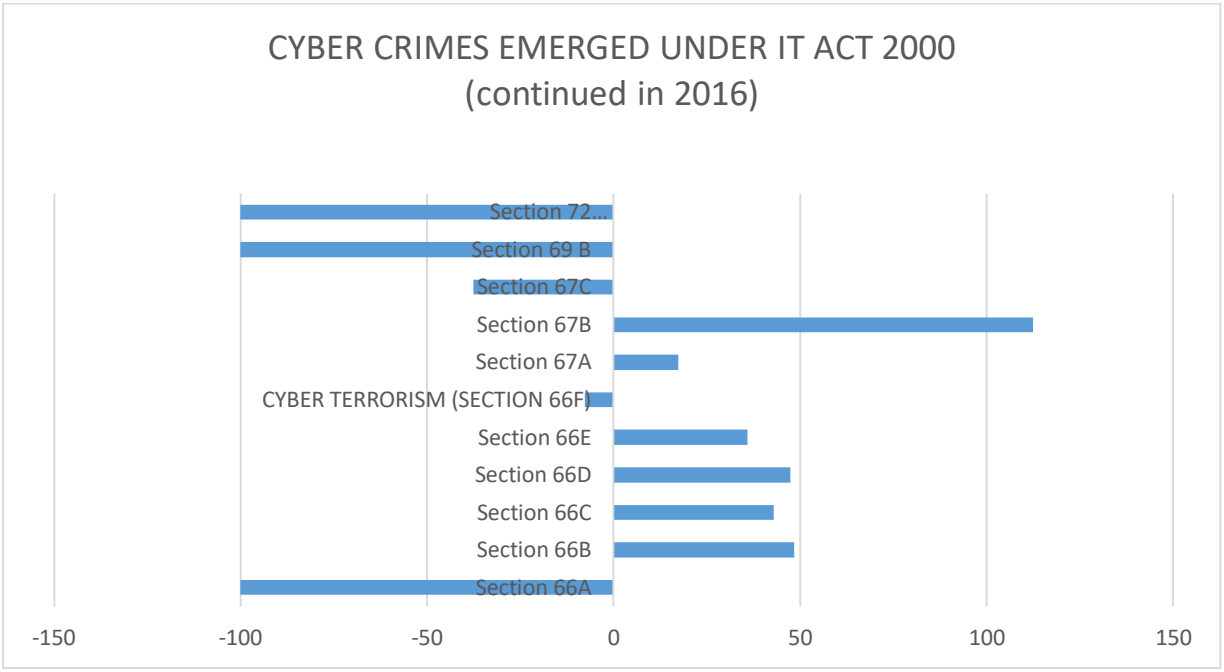


Fig 3.6: Emergent cyber crimes reported under IT Act 2000 in year 2015 and continued in year 2016

Fig 3.6. Represents the emergent types of cyber crimes reported under IT Act 2000 in year 2015 and continued in 2016. It has been noticed that crimes under section 66 and 69A has been emerged to very high growth rate compared to any other crimes recorded in year 2016. Also, it is observed that cyber crimes emerged in 2015 has been continued to occur and became persistent in next year. Table 3.6. Represents the growth rates of emergent cyber crimes under IT Act 2000 in year 2015 but also continued in year 2016.It has been observed that the newly emerged crime is having the first instance of occurrence i.e., in year 2015. Since, it does not have any previous history thus the growth rate of such crime is very large. Also, the growth rate of crimes occurred in previous years has been reduced for section 66A, 66F, 67C, 69B and &72A in year 2016.

Table 3.6: Growth rate of emergent cyber crimes under IT Act 2000 emerged in year 2015 and continued in year 2016

Crime Head / Year	Sec. 66	Sec. 66A	Sec. 66B	Sec. 66C	Sec. 66D	Sec. 66E	Sec. 66F	Sec. 67A	Sec. 67B	Sec. 67C	Sec. 69A	Sec. 69B	Sec. 72A
2016	#	-100	48.48	42.92	47.46	35.89	-7.69	17.42	112.5	-37.5	#	-100	-100

(Source: National Crime Records Bureau website http://ncrb.gov.in/)
(negative % indicates decrease rate of crime, positive % indicates increase rate of crime)
# indicates the larger growth rate (i.e., near to infinity)

3.7 Cyber Crimes under IPC – EMERGENT (2015)

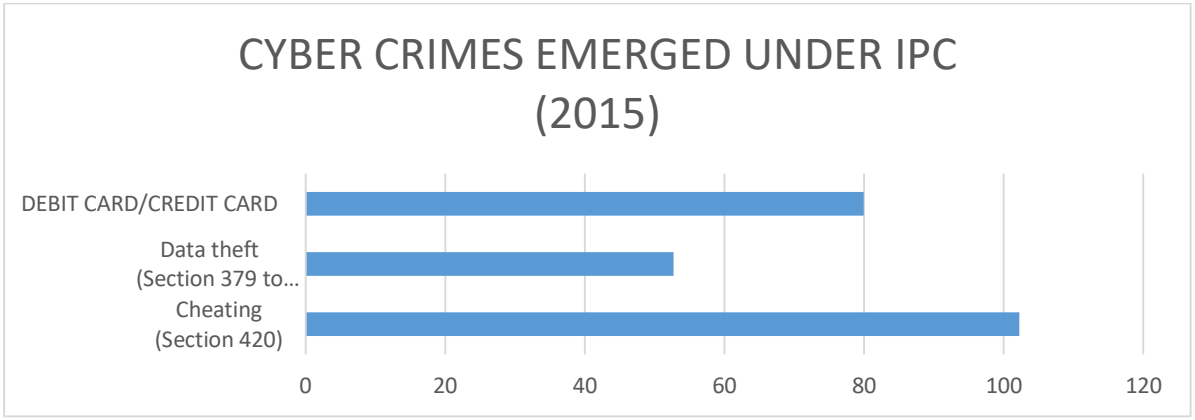


Fig 3.7: Emergent cyber crimes reported under IPC in year 2015

Fig 3.7. Represents the emergent types of cyber crimes reported under IPC in year 2015. It has been noticed that crimes under section 420, 379-381 and frauds related to Credit/Debit cards has been emerged in year 2015. It has been found that there are no cyber crimes recorded under IPC to be emerged in year 2013 and 2014. Table 3.7. Represents the growth rates of emergent cyber crimes under IPC in year 2015. It has been observed that the newly emerged crime is having the first instance of occurrence. Since, it does not have any previous history thus the growth rate of such crime is very large.

Table3.7: Growth rate of emergent cyber crimes under IPC in year 2015

Crime Head / Year	Cheating (Section 420)	Data theft (Section 379 to 381)	Debit card/Credit card
2015	102.2422	52.72727	80

(Source: National Crime Records Bureau website http://ncrb.gov.in/)
(negative % indicates decrease rate of crime, positive % indicates increase rate of crime)

3.8 Cyber Crimes under IPC – EMERGENT continued in 2016

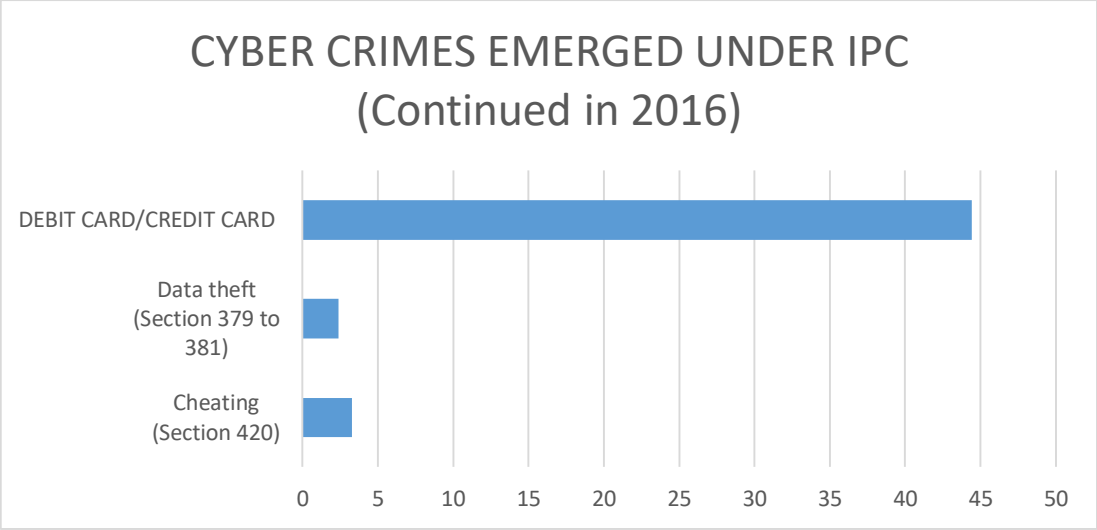


Fig 3.8: Emergent cyber crimes reported under IPC in year 2015 and continued in year 2016

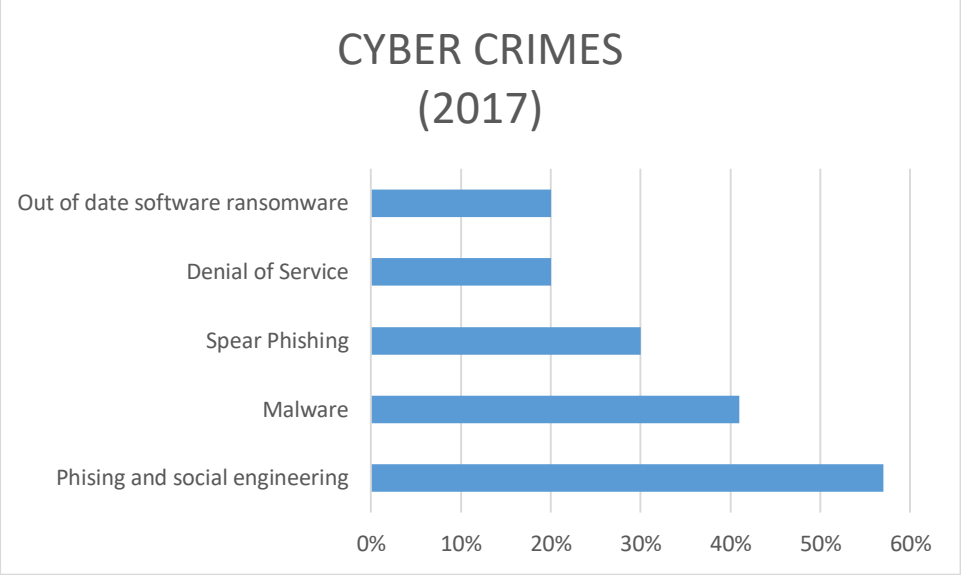
Fig 3.8. illustrates the emergent types of cyber crimes reported under IPC in year 2015 and then continued in year 2016. It is observed that cyber crimes emerged in 2015 has been continued to occur and became persistent in next year. It has been found that there are no cyber crimes recorded under IPC to be emerged in year 2013 and 2014. Table 3.8. Represents the growth rates of emergent cyber crimes under IPC in year 2015 but also continued in year 2016. It has been observed that the newly emerged crime is having the first instance of occurrence i.e., in year 2015. Since, it does not have any previous history thus the growth rate of such crime is very large. Also, the growth rate of crimes occurred in previous years has been reduced for crimes related to cheating, data theft and frauds related to debit/credit card in year 2016.

Table 3.8: Growth rate of emergent cyber crimes under IPC in year 2015 and continued in year 2016

Crime Head / Year	Cheating (Section 420)	Data theft (Section 379 to 381)	Debit card/Credit card
2016	3.281	2.38	44.44

(Source: National Crime Records Bureau website http://ncrb.gov.in/)
(negative % indicates decrease rate of crime, positive % indicates increase rate of crime)

3.9 Cyber Crimes recorded in year 2017



(Source: 'Cyber Security' article published in NITI Aayog)

Fig 3.9: Percentage disruption of cyber crimes in year 2017

Fig 3.9. Illustrates the continuation of emergent of cyber crime occurred in year 2017. Cyber crime disruption has been found for crimes such as phishing, denial of service attack, ransomware software, and malware. Table 3.9. Also illustrates the different types of cyber attacks/crimes reported and continued to occur since 2013 till now.

Table 3.9: Cyber crimes continued to occur since 2013 till now.

Cyber Attacks/crimes (year wise)			
2013	**2014-16**	**2015**	**2017**
Cryptolocker	CryptoWall	TeslaCrypt	WannaCry

IV. PREVENTATION MEASURES

4.1 Cyber crime Prevention Measures by Indian Government:

- Setting up cyber crime cells in different states and Union territories for reporting and investigating the cases of cyber crimes
- Cyber forensic training centers and labs are set up in the States of Kerala, North east India and Jammu & Kashmir
- Cyber forensic training centers and labs are set up for providing awareness and training at cities like Mumbai, Bengaluru, Pune and Kolkata in collaboration with Data Security Council of India (DSCI), NASSCOM
- Training has been provided to all police officers and Judicial officers to handle cyber crimes
- Cyber crime helplines have been set up to provide 24x7 services to report the cyber crime cases
- Set up of Mobile applications to report for cyber crime cases
- Different cyber security websites have been set up to report and resolve the different types of cyber crimes
- Set up of Indian Computer Emergency Response Team (CERT-In) as the national agency for incident response including analysis, forecast and alerts on cyber security breaches
- Framework for enhancing security in cyberspace has been approved with the National Security Council Secretariat as nodal agency for cyber security in the Indian cyberspace

4.2 Few Websites, Social Networking portals and Mobile Applications set up by Government of India:

4.2.1 Websites:

- https://www.cyberswachhtakendra.gov.in/
- https://cyber crime.gov.in/
- https://www.cert-in.org.in/
- https://mha.gov.in/
- https://digitalpolice.gov.in/
- http://www.cybercelldelhi.in/Report.html
- https://www.cyber crimehelpline.com/submit-your-case/

4.2.2 Social Networking Awareness Portals:

- https://twitter.com/ CyberDost
- http://www.tweesurfing.in/
- http://socialsurfing.in/
- https://www.facebook.com/Cyber crimeCellIndia/

4.2.3 Mobile Applications:

- Cyber crime helpline
- MKavach
- Cyber swachhata Kendra
- Cyber crime police station manipur
- Cyber crime clinic
- National Cyber Security

4.3 Best Practices to avoid pit holes:

- Update computer on regular basis by installing and updating antivirus software in computers
- Keeping computer system, password authenticated and keeping a strong password which should have combination of text, special symbols and numbers
- Try avoid using same password in all online services you use
- Do not share personal information like phone number, residential address, bank details etc. to unknown
- Do not respond to fake calls and emails which asks for sharing of personal information
- Pay attention to different websites and software's privacy policies
- Review bank and credit card statements in timely manner
- Do not share fraudulent or fake information
- Do not share personal images, data to anyone on any e-channel
- Do not respond to any email, messages regarding discount or scheme related to holidays, shopping for asking credit and debit card details
- Follow social networking security policies and do not respond to any unknown request
- Do not respond to any phone calls which are stated as bank calls and do not share bank details on those calls first confirm it by visiting respected bank branch
- While visiting any website check for secured protocol version like https instead http

V. CONCLUSION

- It has been concluded that the growth rate of cyber crime increases with the increase in internet usage, in India.
- Persistent types of cyber crimes such as tampering with computer source document, publishing obscene information in electronic form, refusal to decrypt data and to comply with orders, attempting to secure access to a protected system, misinterpretation, breach of confidentiality and privacy, false digital signature certificate publication and fraud digital signature were recorded repetitively in consecutive years under IT Act 2000. Also, crimes such as offences against/by police servant, forgery, criminal breach of trust, counterfeiting and destruction of electronic evidence has been recorded persistently under IPC.
- Persistent cyber crimes are occurring repetitively but not with very high rate, thus these crimes are required to be monitored by government of India and by cyber police officers to prevent and control the occurrence of it.
- Emergent types of cyber crimes are those crimes which are not repetitive but are newly observed. These type of crimes occurs without any prior indication of happening. Crimes using computers such as hacking, publishing of threatening information., cheating, receiving stolen communication device or computer, cyberterrorism, publishing of private images of others, publishing obscene information, publishing images containing sexual acts, child pornography, and identity theft have been emerged under IT Act 2000.Also, crimes like data theft, cheating, and credit/debit card frauds has been emerged at a very high rate under IPC
- It has been observed that the newly emerged crime is having the first instance of occurrence. Since, it does not have any previous history and hence the growth rate of such crime is very high. To handle such incidence, government of India and Cyber officers are required to be updated and keep themselves ready to tackle any new emergent crime at any time in any year.
- As cyber crimes are increasing, Indian government is also taking various awareness and prevention measure initiatives by publishing newspaper articles, radio and television advertisements, by sending an email and text messages to be safe and secure, providing and setting up many mobile applications as well as websites to report the crime, by reaching every single internet user through social networking cyber awareness and reporting portals.

VI. ACKNOWLEDGMENT

I am thankful to Mr. Ashish Sharma, Asst. Manager, Risk & Information Security Management at SBI Life Insurance Co. Ltd. for continuous guidance and support.

REFERENCES

[1] Juneed I. Bilal M. 2017. Cyber crime in India: Trends and Challenges. International Journal of Innovations & Advancement in Computer Science, 6(12): 2347 – 8616

[2] Singh A. Singh B. Cyber Security Policies for Digital India: Challenges and Opportunities. International Journal of Computer Sciences and Engineering, 5(12): 2347-2693

[3] http://ncrb.gov.in/

[4] https://data.gov.in/search/site?query=cyber+crime

[5] http://niti.gov.in/

[6] https://www.iamai.in/

[7] http://dot.gov.in/sites/default/files/itbill2000_0.pdf

[8] http://www.internetlivestats.com/

[9] https://www.statista.com/statistics/255146/number-of-internet-users-in-India/

[10] http://pib.nic.in/newsite/PrintRelease.aspx?relid=132545

[11] https://www.cert-in.org.in/

[12] http://gendermatters.in/2018/07/cyber-crime-reporting-portal/