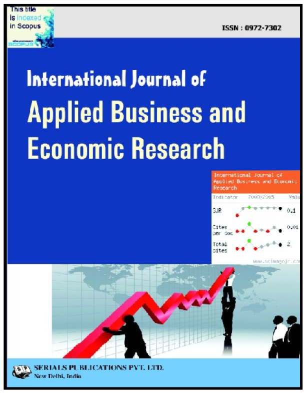

International Journal of Applied Business and Economic Research

ISSN : 0972-7302

available at http: www.serialsjournals.com

© Serials Publications Pvt. Ltd.

Volume 15 • Number 16 (Part - II) • 2017

Analysis of Cyber Safety Awareness Amongst Internet Users in Pune

Swati Sayankar[1] and Asha Nagendra[2]

[1] Research Scholar, Tilak Maharashtra Vidyapeeth, Pune (MH), India
[2] Symbiosis Institute of Management Studies, Pune (MH), India

Abstract: Pune city is growing in all aspects may be Educational, Cultural, Industrial etc. due to its conducive environment. Pune being the IT hub of Maharashtra, has been facing a problem of increasing cyber crimes in last 5 years. This fact is supported by NCRB (National Crimes Record Bureau) of India which has highlighted that Cyber crimes in Pune region are increasing at an alarming rate in the last few years. Hence the need of cyber safety awareness while using Internet or advanced technologies becomes sine-qua-non. The purpose of this research paper was to find out the awareness of Internet Users on cyber safety. For this, primary data was collected and analysed from 1122 people who are using Internet and of are of different age groups. It was found that though people are using new technologies such as Internet, Emails, Social networking sites, antivirus, Debit/Credit cards for financial transactions, they are less aware about the do's and don'ts of using these technologies which is a serious threat to the increasing cyber crimes. There is need to inculcate 'Best Practices' amongst this age group so as to reduce quantum of cyber crimes. If this awareness is not created, the rate of cyber crimes will increase which in turn will create burden on 'Cyber Cell' and 'Cyber Forensic labs'.

Keywords: Cyber safety, Cyber crimes, Netiquette, IT Act, IPC

INTRODUCTION

Cyber crime includes all criminal activities done using the medium of communication devices like computers, worldwide web, mobile phones, tablets, internet and cyber space. Any activity that uses computer as an instrument, target or a means for perpetrating crime falls within the ambit of cyber crime.

Understanding cyber safety is more important when one is online. A person may be a working Professional, Teacher, Parent or family member, the knowledge to stay safe online or while using Information Communication Technology (ICT) is a must.

Cyber safety is the safe and responsible use of information and communication technology. It is about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette). Cybercrime are increasing at an alarming rate. This fact is revealed from the NCRB (National Crimes Records Bureau) of India.

Table 1
Incidence of cases registered under Cyber Crime from 2013-15 under IT ACT (State wise)

SNo	*State*	*2013*	*2014*	*2015*	*Total*
1	Andhra Pradesh	651	282	536	1469
2	Assam	154	379	483	1016
3	Karnataka	533	1020	1447	3000
4	Kerala	383	450	290	1123
5	Maharashtra	907	1879	2195	4981
6	Rajasthan	297	697	949	1943
7	Tamil Nadu	90	172	142	404
8	Telangana	-	703	687	1390
9	Uttar Pradesh	682	1737	2208	4627

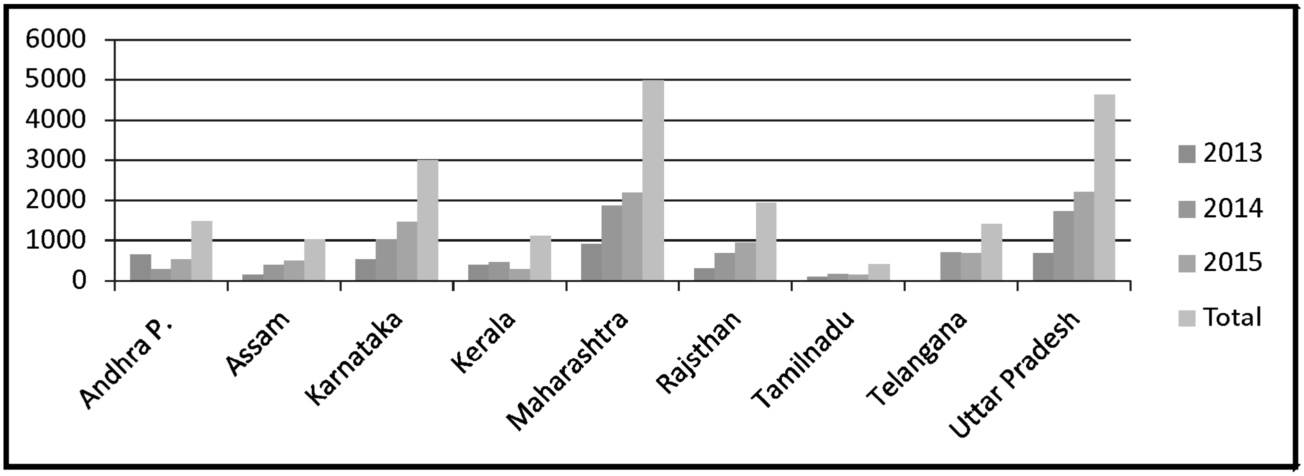

Figure 1: State wise Cyber crimes from 2013-15 in India

The above Table and figure show that in the last 3 years, Maharashtra has the highest no of recorded cyber crimes which is a serious threat to safety and security of Individual, Organisation and state in turn. Pune being the IT and educational hub was therefore considered for the study of cyber safety awareness of people. The observations will help to understand the fact.

REVIEW OF LITERATURE

Report of Cyber Forensic Lab (2009-2011), Santa Cruz (Mumbai)- Maharashtra received from Directorate of Forensic science Laboratories, Home Department, Santa Cruz, Mumbai, Maharashtra under RTI. This report shows trend of rising cyber crimes from 2009 to 2011. The crimes are mostly related to E-mail theft, Data theft, website Hacking, Phishing, Credit card Frauds. There are huge no. of cyber crimes under investigation.

Report of Cyber Cell (2009-2011), Crime Branch, Thane- Maharashtra This report is given by Government Information officer and Asst. Police commissioner, Crime Branch, Thane under RTI. This report highlights cyber crimes related to Data Theft, Phishing, Credit Card Frauds. From 2009-2011, out of 24 cases 16 i.e. approx. 66% cases are under investigation which is a serious threat..

Report of Cyber Crime Cell (2009-2011), Mumbai-Maharashtra received from Cyber Cell, Crime Branch, Mumbai (2012) , given by Government Information Officer and Asst. Police Commissioner, Crime Branch, Mumbai under RTI. This report shows that out of 14 cyber crimes (2009-2011) related to E-mail theft, Data theft, Phishing and Credit Card Frauds, only 4 cases are under investigation which is only 30%.

Report of Cyber Crime Cell (2009-2011), Pune-Maharashtra received from Office of Pune Commissioner and Public Information Officer, Cyber cell, Crime Branch, Pune (2012). This report shows cyber crimes related to Email Threat, Data Theft, Website Hacking, Phishing and Credit card Frauds.

ISO 27001 i.e. ISO27001 is the international Cyber security Standard. It is for managing Information Security System. It provides a prototype for improving, operating establishing, implementing, monitoring, maintaining and reviewing an Information Security System.

Kareem (2015) in his paper on cyber crime investigation, he studies impact of ICT issues on private sectors and e-Governments

Sharma (2012) studied various cyber security emerging trends. These trends he considered as mobile computing, cloud computing, social networking and e-commerce. Dalal (2015) in his research article on Cyber Safety, predicted that state sponsored cyber attacks would increase.

1. OBJECTIVES

1. To identify increasing Cyber crimes in Pune
2. To conduct cyber safety awareness survey of people in Pune
3. To find out probability of risks using Risk assessment Matrix

2. METHODOLOGY

Primary data was collected by the survey method. 2 sets of questionnaires were prepared for collecting data from people.

Questionnaire-1 was filled by personnel from various Cyber cells and Cyber Forensic Lab of Maharashtra for the year 2009-2011.

Questionnaire-2 was filled by the 1122 people of age-group 18-30 on 'Cyber Safety Awareness'.

Questionnaires were designed to study different angles of cyber crime investigation such as frequent cyber crimes, reasons of pending cases, user behaviour while using Internet, Online Banking and other e-transactions, Email, legal aspects etc.

The records of last five years (2011-2016) were collected from various police stations, Cyber Cell in Tabular Format.

Sample size selection was made on the basis of **Morgan table using multistage stratified random sampling.**

Secondary data was collected from the website of National Crime Record Bureau of India.

Data analysis has been performed using **SPSS-21 and Microsoft excel.**

3. AWARENESS OF PEOPLE IN PUNE ON CYBER SAFETY

To identify internet users, the following questions were asked to 1122 respondents.

Q.1) Do you have an email account?

Table 2
Table showing % of Internet users who have email account

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	1065	94.9	94.9	94.9
	No	57	5.1	5.1	100.0
	Total	1122	100.0	100.0	

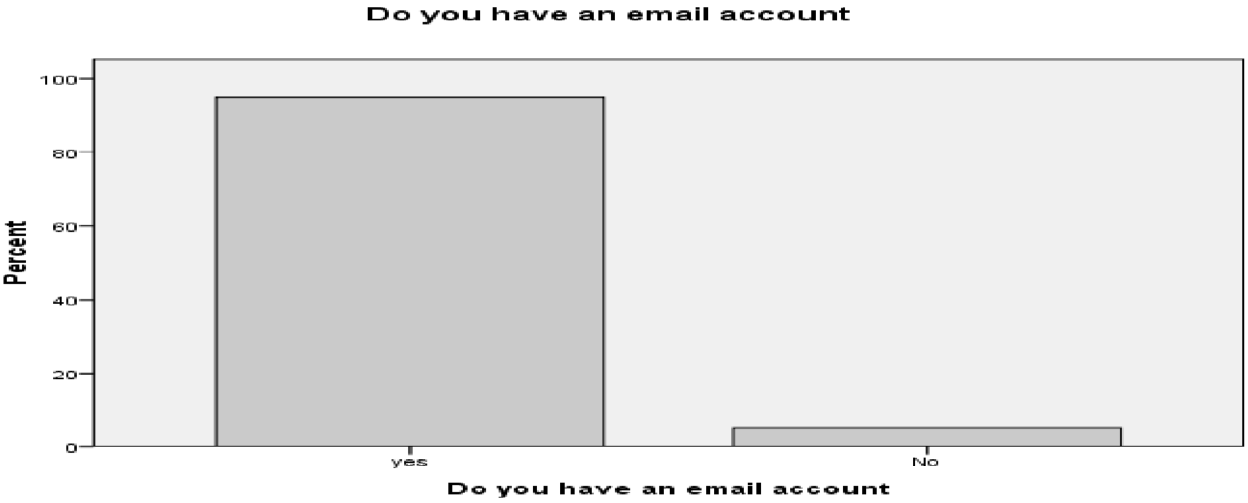

Figure 2: Internet users having an email account

The above frequency distribution table shows that from selected Sample, there are 94.9 % people who are using an email account. Only 5.9% people do not have an email account.

This was the reason why the survey of internet users on "cyber safety awareness" was carried out. Considering various most frequent cyber crimes as reported by NCRB (National Crime Records Bureau of India) related questions were asked to internet users. This will give an idea to researcher about level of awareness amongst internet users.

Q.2) Is your password strong?

Table 3
Strong password

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	Alphabet	267	23.8	23.8	23.8
	Number	176	15.7	15.7	39.5
	Special characters	27	2.4	2.4	41.9
	Alpha numeric	261	23.3	23.3	65.2
	Combination of all	391	34.8	34.8	100.0
	Total	1122	100.0	100.0	

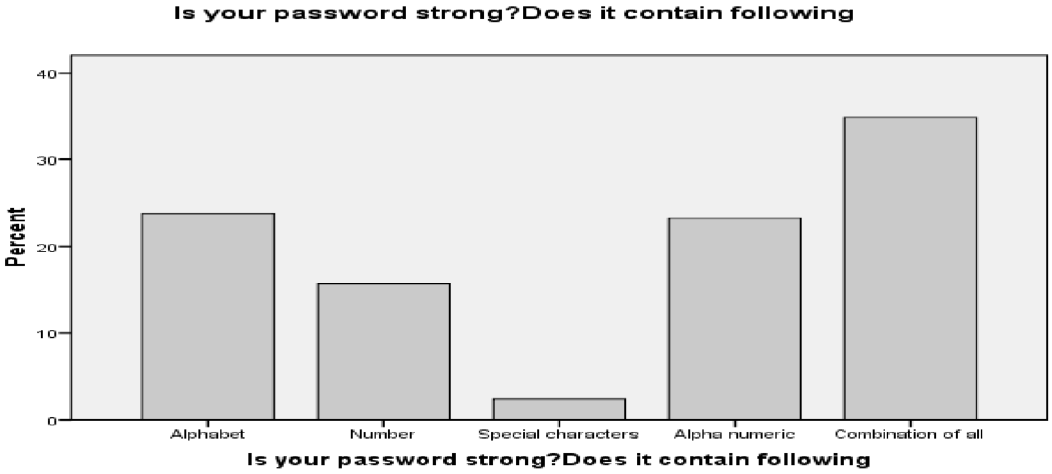

Figure 3: Is your password strong?

From the above figure and table, it can be seen that out of 1065 respondents only 391 users i.e.34.8% people have strong password that contains alphabets, numbers, special characters etc. The strong password is required to protect the system from unauthorised access to data or information. Therefore risk level observed falling to cyber crime is high.

Q.3) Which social networking sites do you use?

Table 4
Use of Social networking sites

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	facebook	529	47.1	47.1	47.1
	twitter	40	3.6	3.6	50.7
	whatsApp	436	38.9	38.9	89.6
	any other	60	5.3	5.3	94.9
	nothing	57	5.1	5.1	100.0
	Total	1122	100.0	100.0	

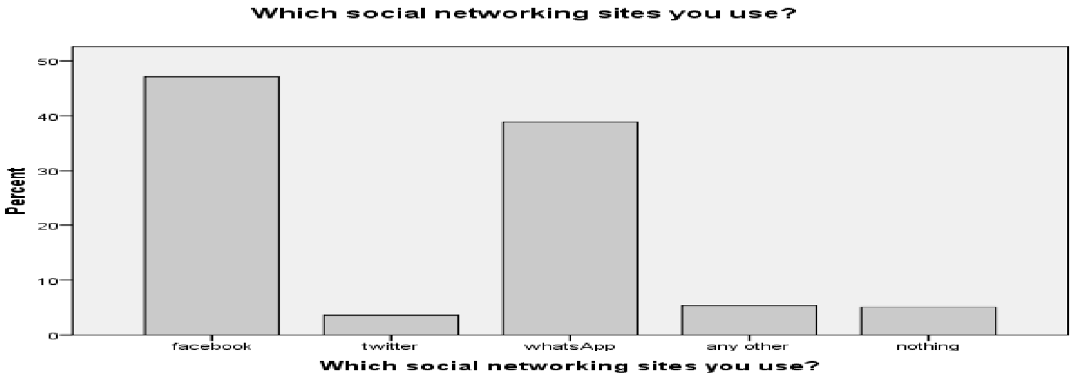

Figure 4 : Use of Social networking sites

From the above frequency distribution table it can be observed that out of 1065 internet users 529 (47.9%) people use Facebook, 436(38.9%) people use WhatsApp and 40 (3.6%) people use Twitter.

It shows that mainly 94.96% people use Facebook, WhatsApp, Twitter and other social networking sites. Hence it becomes necessary to know the Do's and Don'ts while using above media.

Q.4) Do you have different password for email and social media accounts?

Table 5
Different password for email and social media accounts

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	819	73.0	73.0	73.0
	no	303	27.0	27.0	100.0
	Total	1122	100.0	100.0	

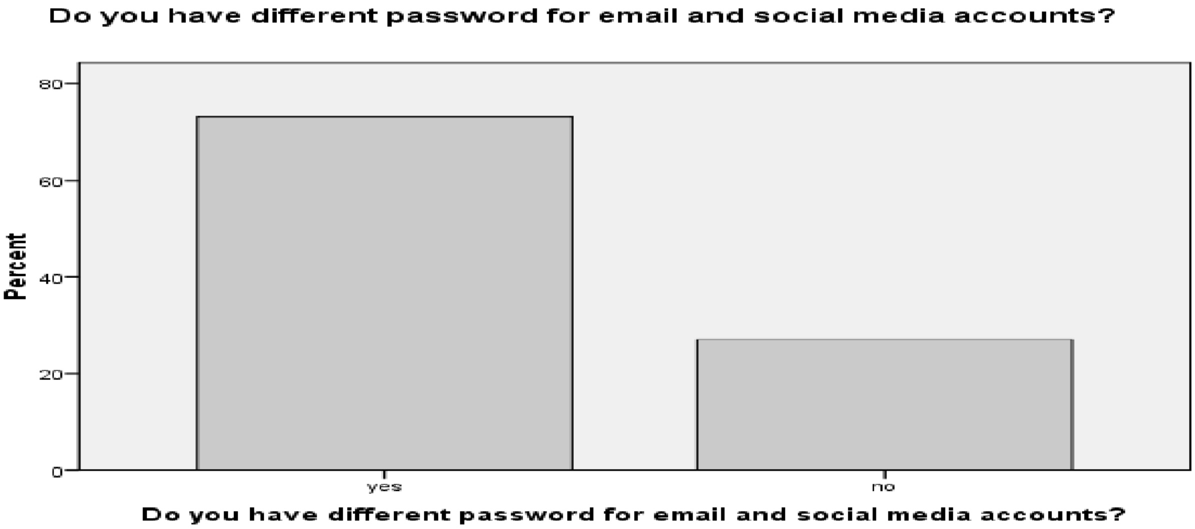

Figure 5: Different password for email and social media Accounts

From the above Frequency table it can be seen that 73% users have different passwords and 27 % users have same password for email and social media accounts which is a threat to cyber safety of these users.

This helps the Hacker to use same password for different accounts and obtain the sensitive information such as Banking details, credit/debit card details, personal information. This may lead to money loss, loss of confidential information of individual or organisation, defamation etc.

Q.5) Have you uploaded following personal details on social networking sites?

Table 6
Personal Details on Social Networking Sites

	Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Your photo	326	29.1	29.1	29.1
contact no.	35	3.1	3.1	32.2
Email	163	14.5	14.5	46.7
Address	12	1.1	1.1	47.8
All	432	38.5	38.5	86.3
Nothing	154	13.7	13.7	100.0
Total	1122	100.0	100.0	

		Frequency	*Per cent*	*Valid Per cent*
Valid	Yes	53	4.7	4.7
	No	815	72.6	72.6
	sometimes	254	22.6	22.6
	Total	1122	100.0	100.0

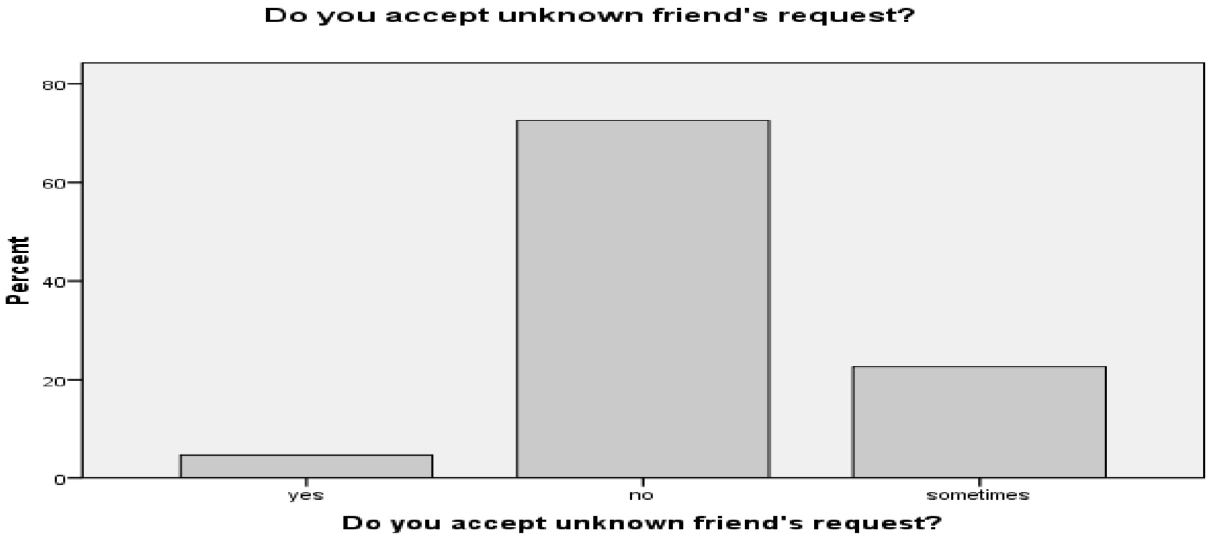

Figure 6: Accepting unknown Friend's Request

From the above Frequency table it can be seen that out of 1122 users, 4.7 % people accept request. 72.6% users not accepting request. But sometimes 22.6% users accept request is a big risk and may fall victim to cyber crimes.

Q.7) Have you installed Antivirus and Firewall on Your PC?

Table 8
Installing Antivirus and Firewall on Your PC

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	installed antivirus only	509	45.4	45.4	45.4
	installed firewall only	35	3.1	3.1	48.5
	installed both-antivirus and firewall	344	30.7	30.7	79.1
	installed none	234	20.9	20.9	100.0
	Total	1122	100.0	100.0	

From above Frequency Distribution Table it can be seen that out of 1122 users 509 users have installed Antivirus, 35 have installed only Firewall and 344 people have installed both. But There are 234 people who have not installed antivirus or Firewall. Therefore it may create big risk as system may fall to data loss, data modification due to virus attack.

Q.8) Do you know IMEI of your mobile Phone?

Table 9
Knowing IMEI of your mobile phone

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	479	42.7	42.7	42.7
	no	643	57.3	57.3	100.0
	Total	1122	100.0	100.0	

Above Frequency Distribution table shows that out of 1122 mobile users, only 42.7 % people know IMEI of their Mobile phone. This is a serious threat as your mobile has important personal and official contact numbers and other files, photos and SMSs.

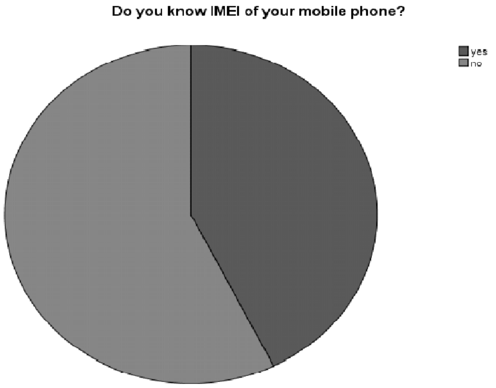

Figure 7: Knowing IMEI of your mobile phone

It can be seen from above graph 57.3 % people do not know IMEI no. of their Mobile. In case of mobile theft or loss of mobile, IMEI no helps Police, Investigation office to track mobile, block the details so that no one can use the data / information from stolen mobile. Hence there is need to create awareness amongst users to know IMEI to save important information stored on Mobile device.

Q.9) Do you note down ATM card and customer service no on your mobile?

Table 10
Noting down of ATM card and customer service number on respondent's mobile?

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	Yes	759	67.6	67.6	67.6
	No	363	32.4	32.4	100.0
	Total	1122	100.0	100.0	

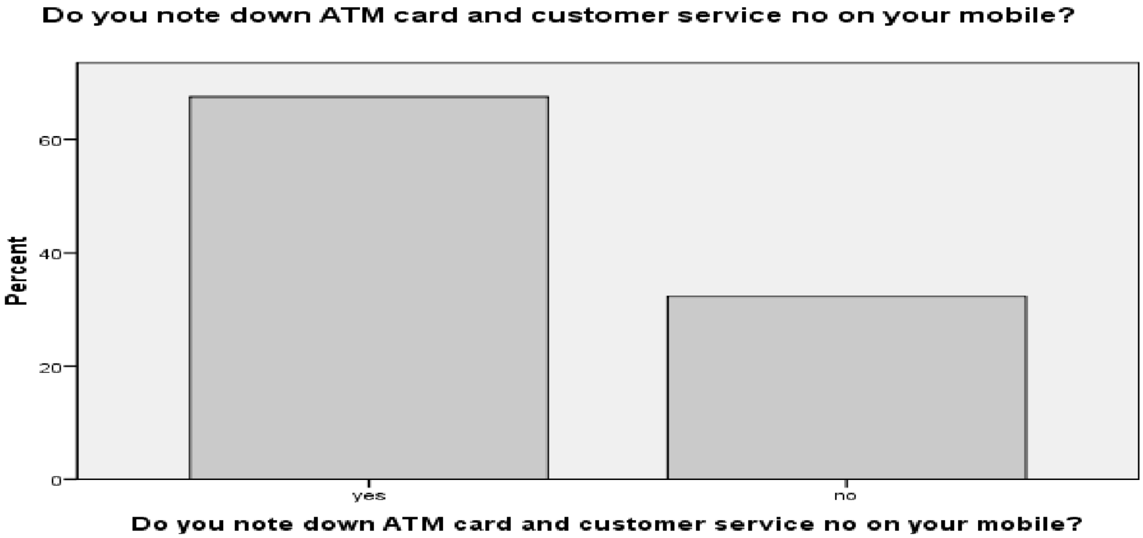

Figure 8: Noting down of ATM card and customer service number on respondent's mobile

Noting down ATM card and customer service number on their mobile may lead to data loss, loss of money through banking transactions.

Q.10) Do you store your password, pin in your mobile as contact number?

Table 11
Storing password, pin in respondent's mobile phone as contact number

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	258	23.0	23.0	23.0
	no	864	77.0	77.0	100.0
	Total	1122	100.0	100.0	

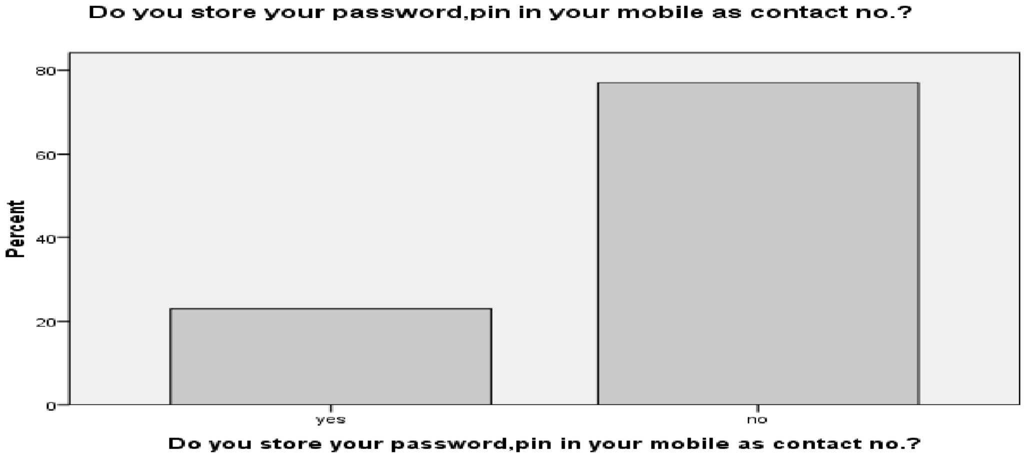

Figure 9: Storing password, pin in the mobile phone as contact number

From the above data, it is seen that 258 people are storing password, PIN on their mobile. This may lead to data loss, loss of money through banking transactions. From Q.9 and Q. 10 it can be observed that storing such sensitive information such as ATM no, Customer service no., password, PIN no is big threat and may lead to cyber crimes.

Q.11) Do you receive email/SMSs / phone calls that promise large sum of money/discounts?

Table 12
Respondents receiving email /SMSs/ phone calls

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	596	53.1	53.1	53.1
	no	526	46.9	46.9	100.0
	Total	1122	100.0	100.0	

Out of 1122 people, 53.1% people are getting such emails /SMSs/ phone calls. This is a significant percentage (being above 50%) and needs special attention and awareness of Individual and Government. The respondents were further asked whether they respond to such mails or SMSs/ phone calls.

Q.11 .1) If Yes, do you respond ?

Table 13
Responding to such calls

		Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
Valid	yes	149	13.3	13.3	13.3
	no	973	86.7	86.7	100.0
	Total	1122	100.0	100.0	

Out of 53.1% people, 13.3 people respond to such emails or SMSs or phone calls. Their method of responding also surveyed further by asking following question.

Q.11.2) If yes, how do you respond?

Out of 266 people, 130 (11.6%) people reply to SMS/email, 60 (5.3 %) people call back to emails or phone numbers or SMSs and 76 (6.8 %) people entertain unknown calls which are a serious threat. They may fall victim to Cyber crimes such as Nigerian Fraud, Phishing scams, Identity Theft etc.

Table 14
Ways of responding to unknown calls

If yes, then how you respond?

	Frequency	*Per cent*	*Valid Per cent*	*Cumulative Per cent*
By replying to SMS/email	130	11.6	11.6	11.6
By calling contact no.given in email/sms	60	5.3	5.3	16.9
By entertaining their call	76	6.8	6.8	23.7
not applicable	856	76.3	76.3	100.0
Total	1122	100.0	100.0	

4. RISK ASSESSMENT TABLE

It is a step in a procedure. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard).

We are specially studying Risk assessment with reference to cyber security. This will help in analyzing factors affecting effective investigation of cyber crimes. There are two types of Risk Assessments·

1) Quantitative Risk Assessment

2) Qualitative Risk assessment

Qualitative risk assessment comes into play when we have the ability to map an amount to a specific risk. Qualitative Risk assessment typically give risk results of 'High', 'Moderate' and 'Low'. By providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization.

Table 15
Risk Assessment Matrix

RISK ASSESSMENT MATRIX			
	H/M/L	H/M/L	H/M/L
MOTIVATION	HIGH	HIGH	LOW
CAPABILITY	HIGH	HIGH	MODERATE
CONTROLS	LOW	MODERATE	HIGH
RISK LEVEL	HIGH	MODERATE	LOW

(P.N. above Risk Assessment Matrix is as per Microsoft's Information Security Standards)

After studying cyber safety awareness various other factors through different questionnaires, following **Risk Matrix** is prepared. This Risk matrix shows Risk levels before and after implementing security measures or Controls.

Risk Assessment Table is based on Microsoft's Risk assessment matrix. This Qualitative Risk assessment typically gives risk results of 'High', 'Moderate' and 'Low'.

By providing the impact, it is possible to adequately communicate the assessment of risk to individual or the organization. This Risk Assessment Table highlights the possibility of cyber crimes based on risk level. This table highlights the fact that there is need to inculcate cyber safety rules awareness amongst users who are using new technologies and internet.

Firstly, the Vulnerabilities are identified. Vulnerability is nothing but a weakness in the system which gives an attacker a chance to attack or hack a system. Based on the responses received from the questionnaire, Risk Assessment Table is prepared.

Table 16
Risk Assessment Table

S.No.	*Vulnerability Gateways for cyber crimes (How it may happen)*	*Yes (%)*	*No(%)*	*Risk level H/L/M*
1.	Strong password (Threat: Majority of the users (65%) do not have strong password.)	34.8	65.2	**H**
2.	Different passwords for email and social networking accounts (Threat: Good to have different passwords. But People may forget passwords. If stored on mobile or database it may be hacked. 27% people are using same passwords which is risk to their social networking accounts)	73%	27	**H**
3.	Accepting Unknown Friends Requests (Threat: Carry risk of personal and social life.)	27.3	72.6	**H**
4.	Installing Antivirus and Firewall both (Need to create awareness amongst 70% people about use of Firewall.)	30.7%	69.3	**H**
5.	Knowing IMEI of your mobile (Helps in Mobile theft. Not knowing IMEI may lead to hack personal information/ Financial loss)	42.7	57.3	**H**
6.	Storing Password / PIN on mobile phone as contact number (In case of mobile theft, details are used by cyber criminals)	23.0	77.0	**M**
7.	Receiving Emails/SMSs/ Phone calls that promise large sums of money /discounts (Gateways for cyber crimes of those who respond)	53.1	46.9	**H**
8.	Responding to such calls	13.3	86.7	**M**
9.	Uploading personal details on Social websites(May lead to personal/ Financial/Social loss)	47.8	52.2	**H**
10.	Way of responding to calls (by SMS/Email/Call/entertain suchcalls)	23.7	76.3	**M**
11.	Accepting unknown friend's request (Risk of cybercrimesincreases)	27.3	72.7	**H**
12.	Noting ATM card and Customer service number on their Mobile phones	67.6	32.4	**H**
13.	**Awareness about terms**			
	Nigerian Frauds	0.6	99.4	**H**
	Credit card frauds	11.1	88.9	**H**
	Phishing	2.7	98.3	**H**
	Identity Theft	5.7	94.3	**H**
	Hacking	38.8	61.2	**H**
	All above (Threat:Very less awareness may give birth to Cyber crimes)	32.8	67.2	**H**

(P.N. Yellow mark highlights risk level High)

Above Risk Assessment Table shows level of Cyber Safety awareness amongst Internet users in terms of Percentage. It is further marked in terms of Risk level which is High or Medium. The percentage highlighted in yellow indicates that there is less awareness related to general awareness while using internet, computers, mobiles, ATM etc. The above table shows that awareness of cyber safety amongst Internet users is less and may give rise to cyber crimes in future.

5. FINDINGS

From above research, following findings have been derived.

1) Majority of respondents (94.5%) now a days are using Internet and email accounts.
2) Password of accounts is not strong amongst 65.2% people.
3) 95% from that use social networking sites
4) 73% respondents use same password for different accounts which is arisk,
5) Almost 48% respondents upload personal details (Photo, Contact number, email, address) on social networking sites which is a risk.
6) Only 45% respondents installed Antivirus on their Computers.
7) 57.13% respondents don't know IMEI of their mobile.
8) 67.6% repondents take a risk to note down ATM and customer service number on mobile.
9) 23% respondents store password, PIN in mobile.
10) 53% respondents receive unknown calls (emails, SMSs, phone calls that promise large sums of money.
11) 23% respondents reply to unknown calls.

6. CONCLUSION

1) Observations on 'Technology awareness' and 'Cyber Security Risk Analysis Report' between the age group of 18-30 based on survey in Pune region reveals that there is a great need to conduct 'Proactive Awareness Campaign' on 'Cyber Safety'.
2) Though people are using new technologies such as Internet, Emails, Social networking sites, antivirus, Debit/Credit cards for financial transactions, they are less aware about do's and don'ts of using these technologies which is a serious threat to increase cyber crimes.
3) There is need to inculcate 'Best Practices' amongst this age group so as to reduce quantum of cyber crimes.
4) If this awareness is not created, the rate of cyber crimes will increase which in turn will create burden on 'Cyber Cell' and 'Cyber Forensic labs'.

This will affect the effective investigation of cyber crimes in Pune region. The period to resolve registered cyber crimes will increase which is a boon for Cyber criminals.

7. MANAGERIAL APPLICATIONS

1) College students can be trained by experts on 'cyber Safety Awareness'. Theses students can conduct presentations in schools and colleges to spread cyber literacy.
2) ERP Software for effective cyber crime investigation process can be developed that will save time for manual work related to cyber crimes investigation and will link all Cyber Cells in the Country.

8. SCOPE OF FUTURE WORK

1. The present research is carried out in Pune region but is must for every city in Maharashtra and also other states of India.
2. Yearly Cyber safety Literacy survey of every city can be done in India.
3. Research on 'Cyber Safety and Security Policies' of different organizations can be done.

REFERENCES

Crime Statistics 2011-2016. (n.d.). Retrieved April 25, 2017, accessed from http://www.ncrb.org

Growing Cyber Security-Industry-Roadmap for India. (n.d.). Retrieved July 20, 2016, from https://www.dsci.in/content/studies-reports

Kadam, A. (2012). Network Security-Defense in Depth. Geographic India System, 35(10), ISSN 0970-647x, 30-31.

Kadam, A. (2012). Physical Security -Defense in Depth. Geographic Information System (GIS),35(11), ISSN 0970-647x, 36.

Kadam, A. (2012). Information Security- Personnel Security-|Defense in Depth. Data Compression,35(12), ISSN 0970-647x, 30-31.

Kothari, C. R., &Garg, G. (2014). Research Methodology-Methods & Techniques(3rd ed., Vol. 3, ISBN:978-81-224-3623-5). New Delhi, Maharashtra: New Age International (P) Ltd.

Mali, P. (2012). Data Loss Prevention (DLP). Geographic Information System (GIS),35(11), ISSN 0970-647x, 35.

Mali, P. (2013). Cyber Law and cyber crimes(1st ed., Vol. 1, ISBN:978-81-8159-574-4). Mumbai, Maharashtra: Snow White.

Mali, P. (2013). Cyber law and cyber crimes(1st ed., Vol. 1, ISBN:978-81-8159-574-4). Mumbai, Maharashtra: Snow white.

Nagpal, R. (n.d.). Evolution of Cybercrimes. Retrieved May 25, 2015, from http://www.cyberlawdb.com/docs/ebooks/cc.pdf

Online Safety Tips. (n.d.). Retrieved June 10, 2016, from http://www.punepolice.gov.in/content/cyber-crime-cell-awareness-notes

Paranjape, V. (2010). Legal Dimensions of Cyber crime and Preventive Laws-with special reference to India(1st ed., Vol. 1). Allahabad, Uttar Pradesh: Central.

Parthsarthi, P. (2012). Cyber crimes. Retrieved January 15, 2016, from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

Sood, V. (2010). Cyber Crime, Electronic Evidence & Investigation Legal Issues(1st ed., Vol. 1, ISBN-978-81-7274-707-7). New Delhi, Uttar Pradesh: Nabhi Publication.

W. (n.d.). Understanding Cyber crimes, Computer Forensics and Legal Perspectives (1st ed., ISBN: 978-81-265-2179). Wiley India Pvt. Ltd.