IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 8 Issue 5, May 2021
ISSN (Online) 2348 – 7968 | Impact Factor (2020) – 6.72
www.ijiset.com

Cyber Security Awareness Campaign Lacking In Rural and Urban Area of India: A Review

[1]Rishesh Kumar Gupta, [2]Abhishek Dewangan

[1]Student of M.Tech 4th Semester in Computer Science Department, Shri Shankaracharya Group of Institutions, Shri Shankaracharya Technical Campus Bhilai, Chhattisgarh-490020, India

[2]Professor, Computer Science Department, Shri Shankaracharya Group of Institutions, Shri Shankaracharya Technical Campus Bhilai, Chhattisgarh-490020, India

Abstract:

The present paper focuses on Cyber Security Awareness Campaign's lacking in rural and urban area of India and our aim is to identify key factors regarding security which may lead them to failing to appropriately change people's mindset and current efforts to improve information-security practices and promote a sustainable society which do not fold to the undesired impact. Critical observations were made over time on the degree of awareness and attitudes of people in some part of rural area of India toward information security. In particular, our work considers these challenges from a knowledge and Psychological perspective. As we believe that understanding how people perceive risks is critical or threat to creating effective awareness campaigns. Changing behavior requires more than providing information about risks and reactive attitude– firstly, people must be able to understand why this is for their own good and follow the best practices, and secondly, they must be motivated and willing to do so, Which can only be achieve by a sustained and effective information security awareness trend. We extract essential components for an awareness campaign also as factors which may cause a campaign's success or failure. Random Interviews were conducted among public using structured questionnaire to elicit information. The outcome showed that most individuals lack adequate on approaches adopted by cyber criminals, and pay little attention to securing their online data.

Keywords. Cyber Security Awareness, Security Awareness, Cyber Crime Safety, Technology awareness, Digitalization, Digital Security awareness.

1. INTRODUCTION:

India has witnessed a 457% rise in cybercrime cases under the Information Technology (IT) Act, 2000 from the year of 2011 to 2016, A recent Assocham-NEC joint study said, Between 2012 to 2017 the numbers of internet users grew by 44 percent. India has seen a series of significant and unprecedented events during the last 3 years, which have brought the issue of cyber security for the Indian Economy which does not limit to any specific sector to the forefront like never before. The most significant factor in this concern has been the ongoing

initiative of the Government of India, through its flagship Digital India program [1] , with a vision to transform India into a digitally empowered society and knowledge economy. The sharp rise in value and volume of digital transactions which affected record levels in March 2017 manifests the accelerated shift towards electronic payments [2]. The continued increase in penetration of inclusive banking through the Pradhan Mantri Jan Dhan Yojana (PMJDY) with the entire number of accounts crossing 29.18 crore [3] , brought the uninitiated and new users into the fold of banking services.

The risk issues and incidents also made their presence felt, major events included the compromise of the SWIFT banking transaction. These raised the bar on the impact of cyber-attacks like never before.

With digitization steps, India is embarking its journey towards digital economy. Digitization brings unmatched functionalities, coverage and usefulness for the massive Indian population. Cyber risk now ranks among the existential risks for Indian banks and it is important that the decision makers treat it as such, if the fruits of digitization have to be reaped and distributed to the Indian citizens the government/system need to ensure that an efficient cyber security awareness program should be carried out with pan India read.

2. TECHNOLOGY LANDSCAPE AND OVERVIEW OF CYBER CRIME, SECURITY AND AWARENESS:

Before going in deep discussion let's understand the basics definition of Cyber World's and related terminologies. This section offers the transparency on various aspects of digital universe which surrounds and affects us knowingly and unknowingly.

I. Definition of Internet :

On 24 October 1995, the Federal Networking Council (FNC) unanimously passed a resolution defining the term Internet. According to it, Internet refers to the worldwide data system that (i) is logically linked together by a globally unique address space supported the web Protocol (IP) or its subsequent extensions/follow-ons; (ii) is in a position to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

II. Cyber space:

A global domain within the knowledge environment consisting of the interdependent network of data information technology infrastructures, including the web, telecommunications networks, computing system's and embedded processors and controllers.

III. **Cyber Crime:**

Cybercrime is that the latest and maybe the foremost complicated problem within the cyber world. "Cyber-crime could also be said to be those species, of which, genus is that the conventional crime, and where either the PC is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a way for perpetuating further crimes comes within the ambit of cyber-crime". A generalized definition of cyber-crime may be "unlawful acts wherein the computer is either a tool or target or both".

(1) The PC could also be used as a tool within the activities like financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, cyber defamation, cyber stalking.

(2) The pc can also be the target for unlawful acts like unauthorized access to computer, computer system, computer networks, theft of data contained within the electronic form, email bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time theft, web jacking, theft of computing system and physically damaging computing system.

Example:- A criminal hacking into a financial institution and routing the accounts half-cents into a separate individual Swiss account. Would be a cyber-crime because the “motive” was to get money for their own personal gain.

IV. **Conventional Crime:-**

Crime or an offence is "a legal wrong which will be followed by criminal proceedings which can result into punishment." The essential characteristic of criminality is that, it is breach of the criminal law. According to LORD ATKIN, "The criminal quality of an act can’t be discovered by regard to any standard but one: is that the act prohibited with penal consequences". A crime could also be said to be any conduct amid act or omission prohibited by law and consequential breach of which is visited by penal consequences.

V. **Cyber-Terrorism**:

There is not a consensus on one definition of cyber-terrorism but all of them specialize that it invokes fear. A 2008 NATO document defines cyber-terrorism as: “a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal.” Another definition from the National Information Protection Center (NIPC) that exists within the Department of Homeland Security (DHS) is: “a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.” The similarities between the two definitions are that cyber-terrorism’s motive is to invoke fear to intimidate a society into changing for the purpose of an ideological goal. Example:- if a terrorist organization was to hack government officials’ personal emails, access contact information and other Personal Identifiable Information (PII) and put this data available online for the world to ascertain and threaten to try to to so to other officials if they are doing not change the present National clean water policies.

VI. **Cyber Criminals:**

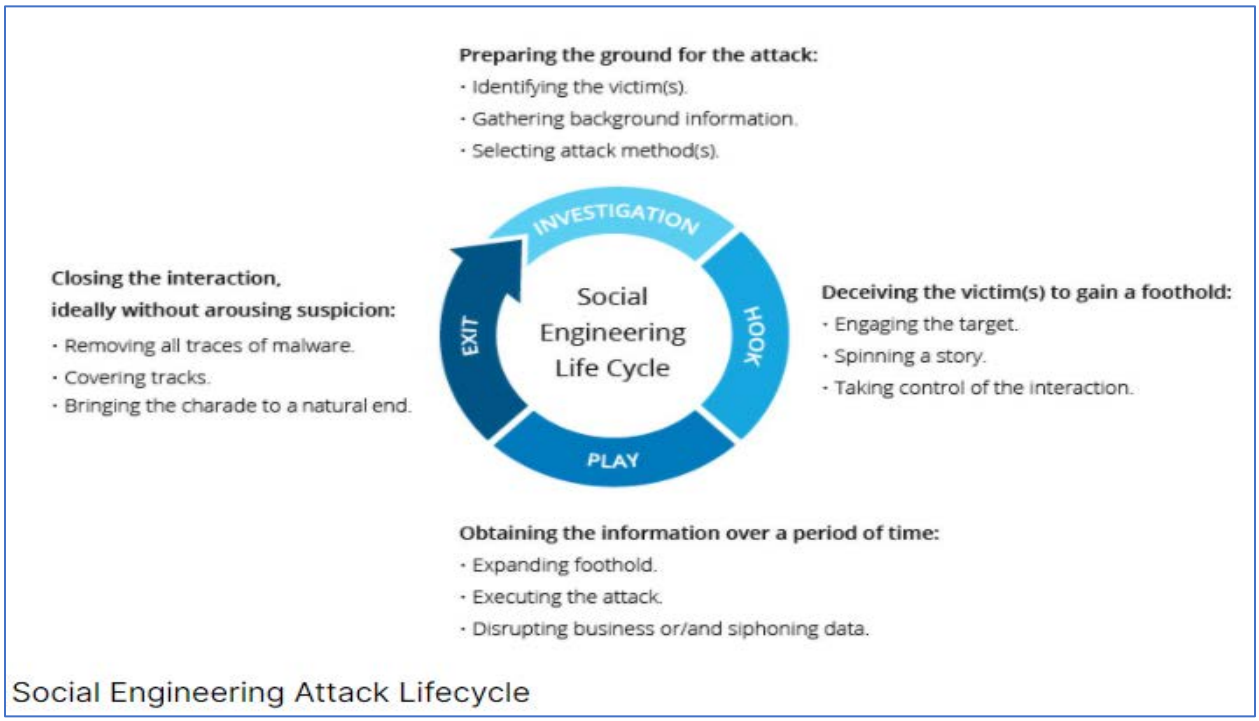
A cybercriminal may be a one that conducts some sort of criminality using computers or other digital technology like the web/Internet**.**

VII. **Phishing:**

It is a kind of social engineering attack often want to steal user data, including login credentials and mastercard numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

VIII. **Social Engineering:**

Social engineering is that the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps [04].



Social Engineering Attack Lifecycle

IX. **Scam:**

It is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.

X. **Victims:**

A person who has suffered physical or emotional harm, property damage, or economic loss as a results of a crime.

Today India is rank 3rd in terms of the very best number of internet users in the world after USA and China. Daily the demand is continually rising, speed of microprocessor chips doubles every 12-18 months, Storage density and bandwidth is doubling every 12 months. Below images showed the expansion of internet users is late 80's to Today.

Some Cyber Crime News articles links mentioned below:

I. Fake' online friend targets state officers for money [22].

II. Private bank staffer, aide held in data theft case[23]

III. Lucknow: Businessman loses Rs 52 lakh to cybercrime; cops say email hacked[24]

IV. Cybercrime sleuths bust 'con call centre'[25]

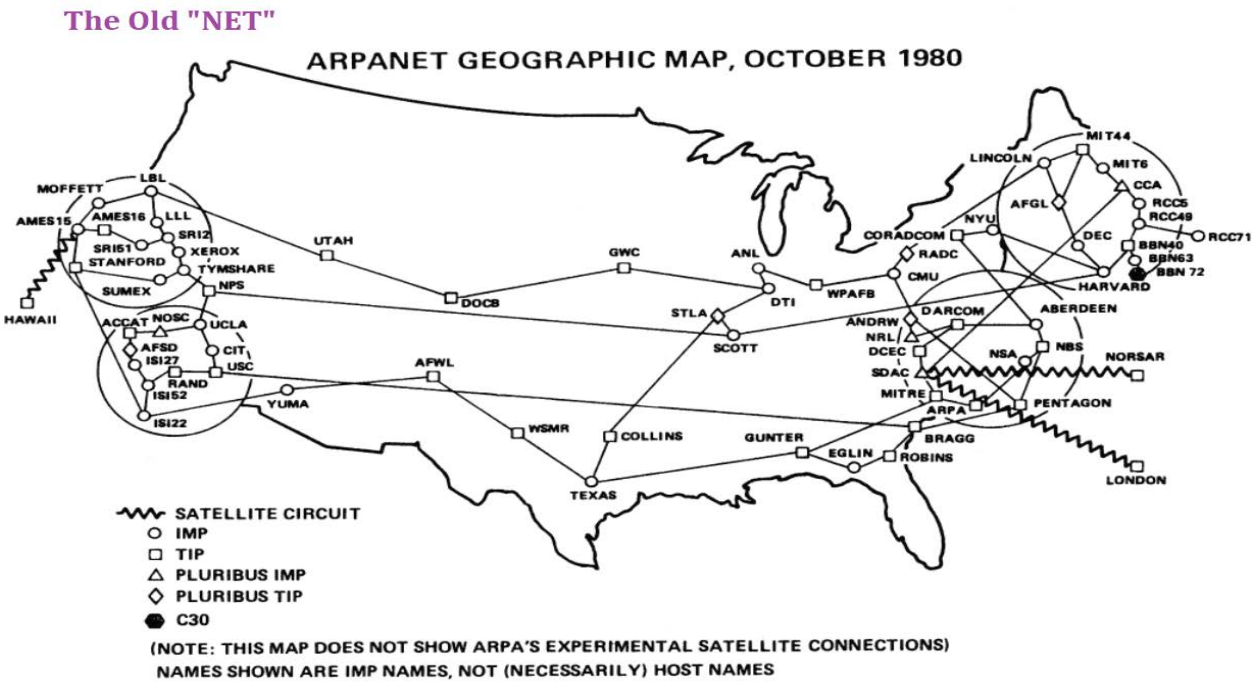
V. Cyber criminals target govt scheme beneficiaries in AP [26]

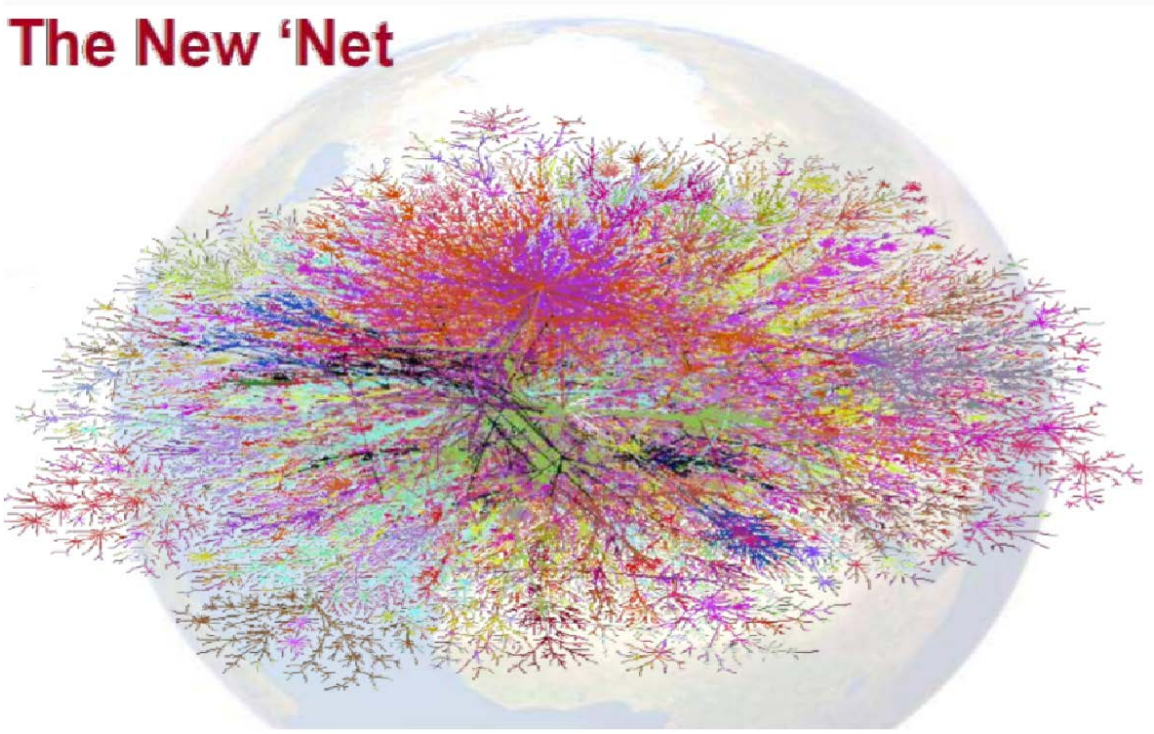
VI. Three held for hacking Bidari's account [27].

VII. Pune: Crooks record video calls to blackmail victims for money [28].

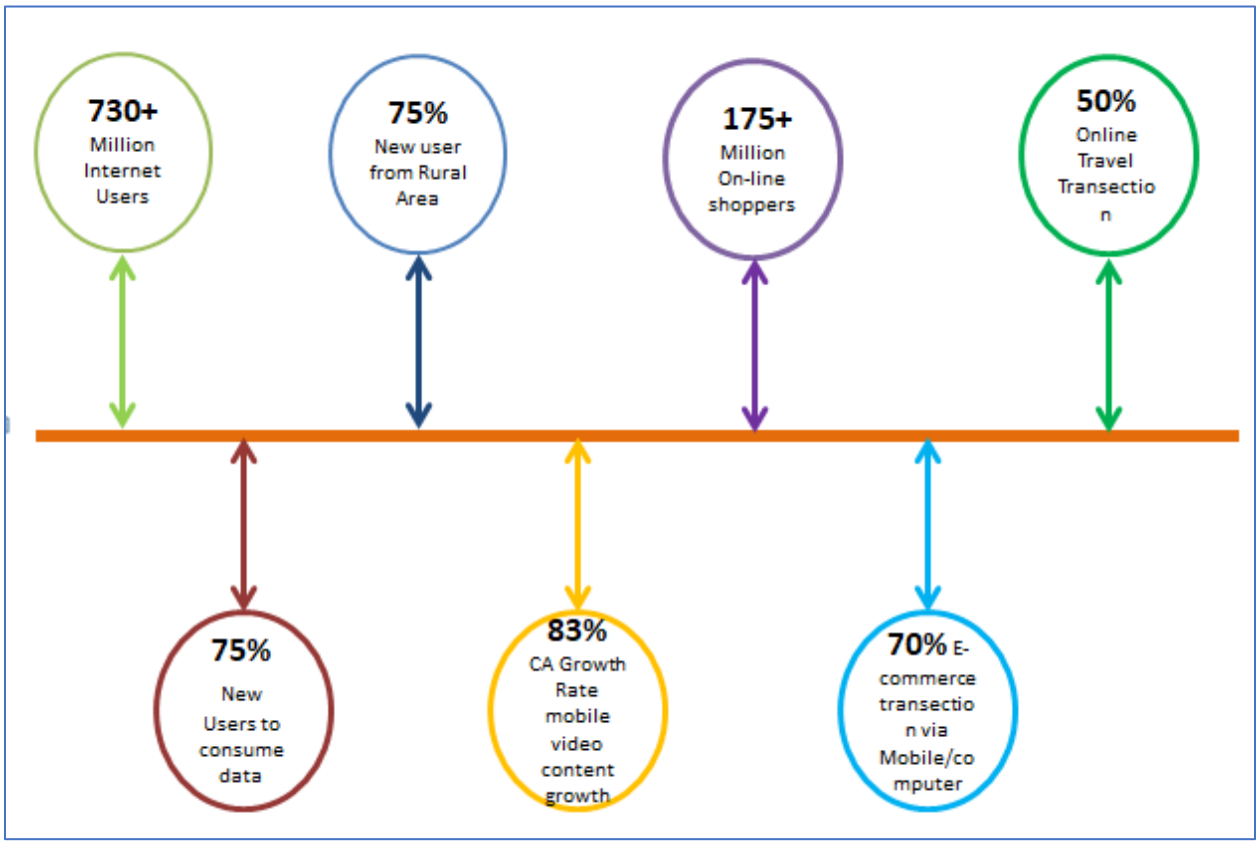
VIII. Rise in cyber attacks during COVID-19 [29].

The internet is growing day by day and daily thousands of internet user's as well. The growth of internet and its user in India by 2020-21





The below image shows the expansion of Cyber World till 2020.



Cyber Security is protecting our cyber space (Critical infrastructure) from attack and damage.

India was ranked among the highest five countries to be suffering from cybercrime, according to a 22' October'2020 report by online security firm "**Symantec Corp**".

3. FACTORS INFLUENCING CHANGE IN CYBER SECURITY AWARENESS BEHAVIOR:

About a third of India's 252 million internet users and a fourth of mobile internet users are in rural areas. But internet penetration in villages, at 8.6% compared to 37.4% in cities, has a long way to go, and this is the statistic 'Digital India' hopes to change. As per a World Bank report, a 10% increase in a country's broadband connections leads to a 1.38% rise in its gross domestic product. Humans are the weakest link in any cyber defense strategy. The process of cyber awareness training is filled with challenges. So, an awareness and educational program is crucial, in that, it's the vehicle for disseminating information each one users (employees, consumers and citizens, including managers) need. The primary purpose of cyber security-awareness campaigns is to influence the adoption of secure behavior. However, effective influencing requires more than simply informing people about what they should and should not do: they need, first of all, to accept that what information is relevant, secondly, understand how they ought to respond. There are many potential reasons for this, but two of the foremost compelling are that people aren't conscious of (or don't perceive) the risks or, they do not know why it is required.

As per my ongoing research i found below points are influencing people behavior.

A. <u>Remote location(Geographical) :</u>

In India many peoples leave in villages doing their traditional work like farming and the villages are still not developed and don't have electricity and Internet connectivity.

B. **<u>Lack of Education/guidelines information awareness :</u>**

In the recently released survey(Sep'2020) by the National Statistical Office (NSO) overall literary rate of India stood at 77.7% and we look state wise the percent Andhra Pradesh 66.4,

Assam 85.9,Bihar 70.9, Chhattisgarh 77.3, Delhi 88.7, Gujarat 82.4,Haryana 80.4,Himachal Pradesh 86.6, Jammu & Kashmir 77.3, Jharkhand 74.3, Karnataka 77.2,Kerala 96.2, Madhya Pradesh 73.7,Maharashtra 84.8,Odisha 77.3,Punjab 83.7, Rajasthan 69.7, Tamil Nadu 82.9, Telangana 72.8, Uttarakhand 87.6, Uttar Pradesh 73.0, West Bengal 80.5[14]. Still many rural area are not educated because of the financial and connectivity issue.

C. **Dynamic Technological Changes:**

Mobile devices and Apps: As organizations move towards adopting mobile devices as its preferred channel for doing business, Many companies are now adapting day by day new technologies for example: After demonetization in India, many finance company came with new way to transfer money via Wallet money transfer and BHIM UPI and still illiterate and less educated are having trouble to operate the application. It also becomes the perfect choice for hackers to take advantages of base increases. Since financial transactions are often done on mobile apps, the mobile phone is becoming a beautiful target resulting in a rise in mobile malware. The risk of jail-broken and rooted devices used for financial purposes increases the scope of attack.

D. **Improper ground level Planning:**

There are no proper guidelines to design and conduct the awareness program in grass root level or community level. The main factor of failing the awareness program because of is not design according to level of people understanding. The key factors are language and region of explanation “WHY, WHEN, WHOM TO ASK”.

E. **Lack of Community Level awareness Program:**

I have visited many remote locations and discussed with rural area public and found that nothing is going on ground level in terms of cyber Security awareness program using banners, posters, street arts, street play etc.

F. Cyber Security Budgets :

Cyber security is an area that affects businesses of all sizes, including small businesses. In fact, about half of all cyber-attacks target small businesses and 68% of small businesses have experienced a cyber-attack in the last 12 months [32]. Company is and the Business both are growing but budget are either Low or constant.

G. **Lack of Cyber Volunteers across the states in the country:**

Country is growing so do the city but in the Rural area are still developing slowly and peoples are not aware about the cyber security and there is not a single person as cyber security volunteer who can help the and advise them to what to and what not to do. Still government is launched the program but its only available for selected states like: **Delhi, Rajasthan, Uttarakhand and Chhattisgarh** [30].

H. **Fake News**:

Social Media, Growing adoption of social media results in more potential for hackers to take advantage of. Many users puts his/her data out on social media like Facebook, Instagram, for anyone to see, which can be potentially exploited to attack the user's organization. Use of social media to propagate fake news can impact banks' reputations in an insidious manner.

4. A SURVEY ON AWARENESS RESPONSE

A blind survey was conducted between age group of 15 ~ 55 to elicit facts about the level of awareness toward cyber security. Critical observations made by visiting in different -2 states and also visiting some organization that provide related services mediated over the Internet to the public. The identities of those interviewed as well as the organization contacted were not sought for in order to avoid infringing on their security rights to enable freedom expression without being held liable for divulging some critical information. The research was conducted in Assam, Bihar, Chhattisgarh, Jharkhand, Madhya Pradesh, Uttar Pradesh, Maharashtra, Gujarat, Haryana, Karnataka, Punjab, Rajasthan, Telangana, Tamil Nadu and Uttarkhand.

A Set of questionnaires requiring YES/NO response were administered in each of the areas: One was to test the degree of awareness of individuals on cyber security while the others was to test their attitudes towards the security of their data (whether they show laxity or seriousness). Each response option with the highest number of respondent as the opinion to uphold.

5. CONCLUSION

The main aim of this paper is to identify the gap between delivery method of cyber security awareness program and targeted audience (Public).

The objectives that are specified in this paper mentioned as to Review the strategies adopted by criminals in exploiting their Victims and Determine the level of awareness of individuals on cybercrime strategies and their attitudes toward information security with the help of information (data) gathered by blind survey in public places (different-2 Cities/villages of India) .

This study has initiated a pioneering effort on real time cyber security awareness by providing some data and information security tips. A review of the level of awareness of individuals and organizations on cyber security as well as their attitudes towards securing their data. Also the strategies adopted by cyber criminals to succeed have been reviewed to provide information on how to guide against falling prey to hackers. It has been observed that majority of are unaware of the risks their data and information are exposed to the social media platform and this also informs why most of them devote little attention to adopting data/information security strategies, thus making them prone to cyber-attacks.

REFERENCES

1. http://digitalindia.gov.in/content/about-programme
2. http://indianexpress.com/article/business/banking-and-finance/demonetisation-fallout-after-a-dip-in-jan-and- feb-digi-payments-rising-4646842/

3. https://www.pmjdy.gov.in/account accessed on 29 July, 2017
4. https://en.wikipedia.org/wiki/
5. https://www.tandfonline.com/doi/abs/10.1080/0144929x.2012.708787
6. https://www.tandfonline.com/doi/full/10.1080/0144929X.2011.632650?src=recsys
7. https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
8. https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security
9. https://www.indusface.com/blog/digital-india-cybersecurity/
10. https://idsa.in/system/files/book/book_indiacybersecurity.pdf
11. https://apwg.org/blog-roll/
12. https://www.first.org/
13. https://www.timesnownews.com/education/article/international-literacy-day-2020-andhra-pradesh-worst-delhi-2nd-best-state-wise-literacy-rate-in-india/649224
14. https://www.tessian.com/blog/phishing-statistics-2020/
15. https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/
16. https://apwg.org/about-us/
17. https://www.researchgate.net/publication/271298620_A_Cyber_Era_Approach_for_Building_Awareness_in_Cyber_Security_for_Educational_System_in_India
18. Maria Bada, Angela M. Sasse, Jason R. C. Nursehttps://arxiv.org/abs/1901.02672#:~:text=Changing%20behaviour%20requires%20more%20than,changes%20to%20attitudes%20and%20intentions.
19. https://blog.hootsuite.com/simon-kemp-social-media/
20. https://www.pwc.in/press-releases/2020/significant-rise-in-cyber-incidents-as-hackers-exploit-the-covid-19-crisis-pwc-india.html
21. http://timesofindia.indiatimes.com/
22. (https://timesofindia.indiatimes.com/city/goa/fake-online-friend-targets-state-officers-for-money/articleshow/82169666.cms)
23. https://timesofindia.indiatimes.com/city/pune/pvt-bank-staffer-aide-held-in-data-theft-case/articleshow/81957640.cms
24. https://timesofindia.indiatimes.com/city/lucknow/bizman-loses-rs-52l-to-cybercrime-cops-say-email-hacked/articleshow/81878936.cms
25. https://timesofindia.indiatimes.com/city/ahmedabad/cybercrime-sleuths-bust-con-call-centre/articleshow/81788899.cms
26. http://timesofindia.indiatimes.com/articleshow/81694144.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
27. http://timesofindia.indiatimes.com/articleshow/81442535.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
28. http://timesofindia.indiatimes.com/articleshow/81338098.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
29. https://www.pwc.in/press-releases/2020/significant-rise-in-cyber-incidents-as-hackers-exploit-the-covid-19-crisis-pwc-india.html
30. https://cybercrime.gov.in/Webform/CyberVolunteerinstruction.aspx
31. https://www.meity.gov.in/writereaddata/files/Cyber-Surakshit-Bharat-Brochure.pdf
32. https://www.mdsny.com/the-cost-of-cybersecurity-and-how-to-budget-for-it/

Author Profile

	**Rishesh Kumar Gupta,** Student of M.Tech 4th Semester in Computer Science Department, Shri Shankaracharya Group of Institutions, Shri Shankaracharya Technical Campus (Approved by AICTE, New Delhi, India) Bhilai, Chhattisgarh-490020, India
	**Abhishek Dewangan, M.Tech** Professor, Computer Science Department, Shri Shankaracharya Group of Institutions, Shri Shankaracharya Technical Campus (Approved by AICTE, New Delhi, India) Bhilai, Chhattisgarh-490020, India