iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37446

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

A Solution Paper on Cyber Security Awareness Campaign Lacking in Rural and Urban Area of India

Rishesh Kumar Gupta[1], Abhishek Dewangan[2]
[1, 2]*Shri Shankaracharya Group of Institutions, Bhilai*

Abstract: ***The present paper focuses on Cyber Security Awareness Campaign's lacking in many rural and urban area of India and Changing behavior requires more information security awareness programs and we extract essential components from Social media and with appropriate procedural and technological work. We can use it for an awareness campaign. Large amount of raw data that has been viewed by users in the form of text, videos, photos and audio. The outcome showed that the delivery methods improves the awareness on the general population.***

Keywords: Cyber Security Awareness, Security Awareness, Cyber Crime Safety, Technology awareness, Digital Security awareness etc.

I. INTRODUCTION

India is a growing country in all aspects and so do the other things are also growing like Technology and modernizations of living as well. The Technology is the key factor of development of any country. In 2015 Indian Government. realized and started massive campaign to uplift the usage of technology in India. The objective was to form the Government services easily available to the citizens electronically by improving its online infrastructure everywhere the country. The process would be structured to extend internet connectivity to form the country digitally empowered. It helps to succeed in bent the masses and encourage them to use technology in their daily lives. Honorable Prime Minister Mr. Narendra Modi launched the campaign on Dominion Day , 2015. The initiative aims at connecting rural India with the assistance of high-speed internet connectivity.

The usage of internet increase so do the crimes also getting increased and it changed the way it was, now many criminals are using technology for frauds and crime. The NCRB's data stated that 4,4546 cases of cyber crimes were registered in 2019 as compared to twenty-eight thousand twenty eight in 2018. The data showed in 60.4 percent of cases, registered fraud was the motive followed by sexual exploitation (5.1%) and causing disrepute (4.2%). Highest number of cyber crime cases were registered in Karnataka (12,020) followed by Uttar Pradesh (11,416), Maharashtra (4,967), Telangana (2,691) and Assam (2,231). Among the Union Territories, Delhi alone accounted for 78 percent of cyber crimes.

As per the info , in metropolitan cities, a complete of 18,372 cases were registered, showing a rise of 81.9 percent. The data also stated maximum cases (13,814) were registered under computer related offenses (section 66 of IT Act).

II. TECHNOLOGY OVERVIEW

Workplaces rapidly shifting to digitally enabled business solutions, education and medical consultations going online, and contactless digital transactions being preferred and promoted are just a few examples of how technology is quickly establishing a ubiquitous presence. India is improving in technology and the risk of digital security is also increasing. "More the digitisation, more frauds will be highlighted that's why numbers have spiked up so much". Let understand the basic terms in the technology, cyber crime and security.

A. 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".

©IJRASET: All Rights are Reserved

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.

B. 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.

C. Cyber-Terrorism

There is not a consensus on one definition of cyber-terrorism but "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".

D. Cyber Criminals

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

E. 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.

F. 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].

G. Scam

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

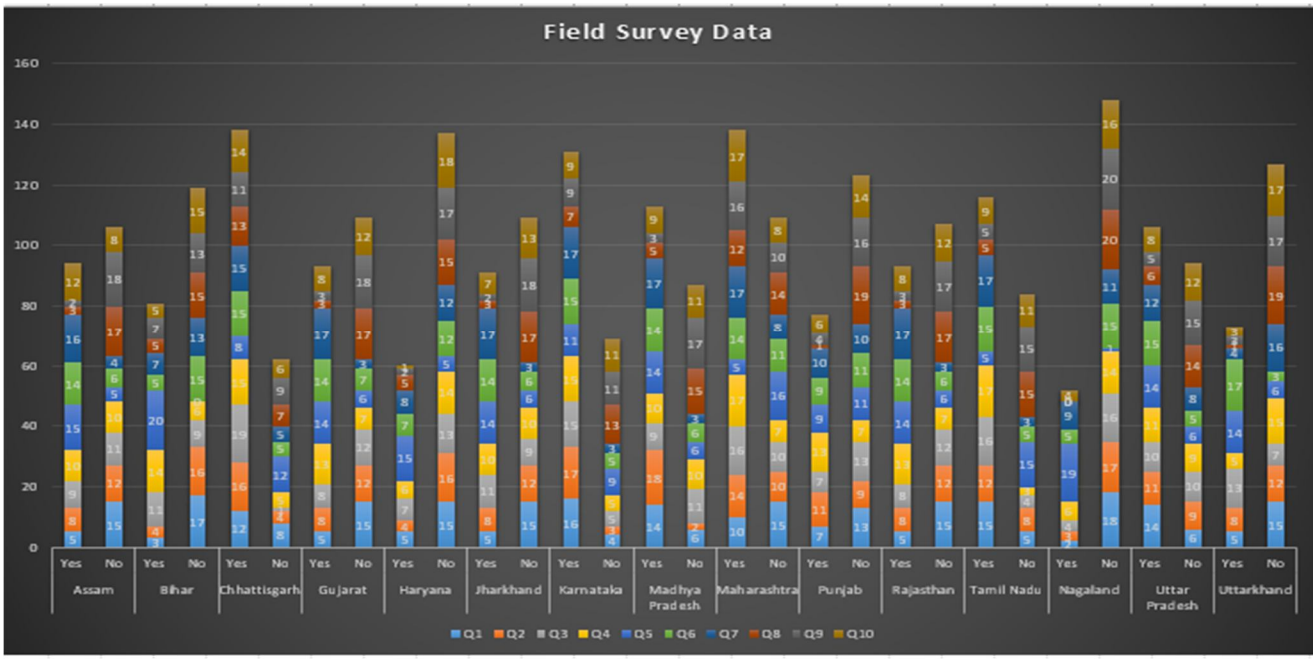
H. Victims

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

III. 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 several states and also visiting some organization that provide related services mediated over the web to the general 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 of 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. As I have collected the answer on the basis of predefined set of questions. These questions are related to general people's daily activity. By the help of general survey I have recorded the public answer and converted into survey graph for better understanding and presentation prospective.

©IJRASET: All Rights are Reserved



IV. SOLUTION

After conducting a blind survey in general public as well as on working professional in technology field we analyze the survey paper and we discussed with the peoples to understand what is there understanding toward data security, privacy cybersecurity and awareness. The outputs are very shocking as they don't have any major concern because they don't know what can be happen if there information publicly available. This is happening because lack of digital literacy.

As Government. is launched digital India campaign in order to ensure the Government's services are made available to citizens electronically by improved online infrastructure and by increasing Internet connectivity or making the country digitally empowered in the field of technology but still need to explain in brief (by adding the awareness with real life or day to day activity examples). By the help of pictorial (photo/posters) and cinematic (Video) campaign because a large amount information is easily can deliver by the help of social media and public prefer to watching instead of reading.

V. CONCLUSION

In this paper we have discussed about how India is growing in all aspect and the technology is the key factor of development. In 2015 Indian Government realized and started massive campaign to uplift the usage of technology in India. The objective was to form the Indian Government services easily available to the citizens electronically by improving its online infrastructure everywhere the country. In this way Government has launched many programs to increase digital literacy in country wide.

"More the digitisation, more frauds will be highlighted that's why numbers have spiked up so much".

India becomes favorite destination for cyber criminals and they are using many techniques like online scam, phishing, Social Engineering to manipulate people because they don't have technology knowledge and the become victims.

To test the knowledge of general public I did a field survey with the set of question to test their knowledge and understanding toward digitalization, technology awareness and challenges they are facing during adapting the changes. The above graph represent the data of peoples understanding.

The main challenge as I understand after discussion is Education, language, poverty and no responsible representor who can present or explain the various benefits and programs run by the Government of India. As we all well aware that human memory is to capture the images, moments and instances long time instead of storing written information. So we give some awareness knowledge by two way.

1) Provided the document for best practices to handle there password, ATM Password etc.
2) We played a small video to understand their degree of understanding and awareness.

©IJRASET: All Rights are Reserved

VI. FUTURE WORK

Current paper work is to identify the gaps in delivery methods currently in use. For the future work we are exploring and refining the delivery methods to increase and deliver the awareness to the general public. The method that use to delivery any information, awareness to general public and they can understand without hesitation, language barrier and any dependency.

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://ncrb.gov.in/
[6] https://cybercrime.gov.in/Webform/CyberVolunteerinstruction.aspx
[7] https://www.mdsny.com/the-cost-of-cybersecurity-and-how-to-budget-for-it/
[8] https://www.tessian.com/blog/phishing-statistics-2020/
[9] https://www.cioandleader.com/article/2020/07/13/india-third-most-cyber-attacked-country
[10] https://www.meity.gov.in/about-meity/organization-chart
[11] https://www.ndtv.com/india-news/digital-india-sees-63-5-increase-in-cyber-crime-cases-shows-data-2302958
[12] https://cybercrime.gov.in/
[13] https://www.forbes.com/sites/ronakdesai/2020/05/14/cybercrime-in-india-surges-amidst-coronavirus-lockdown/?sh=2bd4f834392e

Author Profile



Rishesh Kumar Gupta,

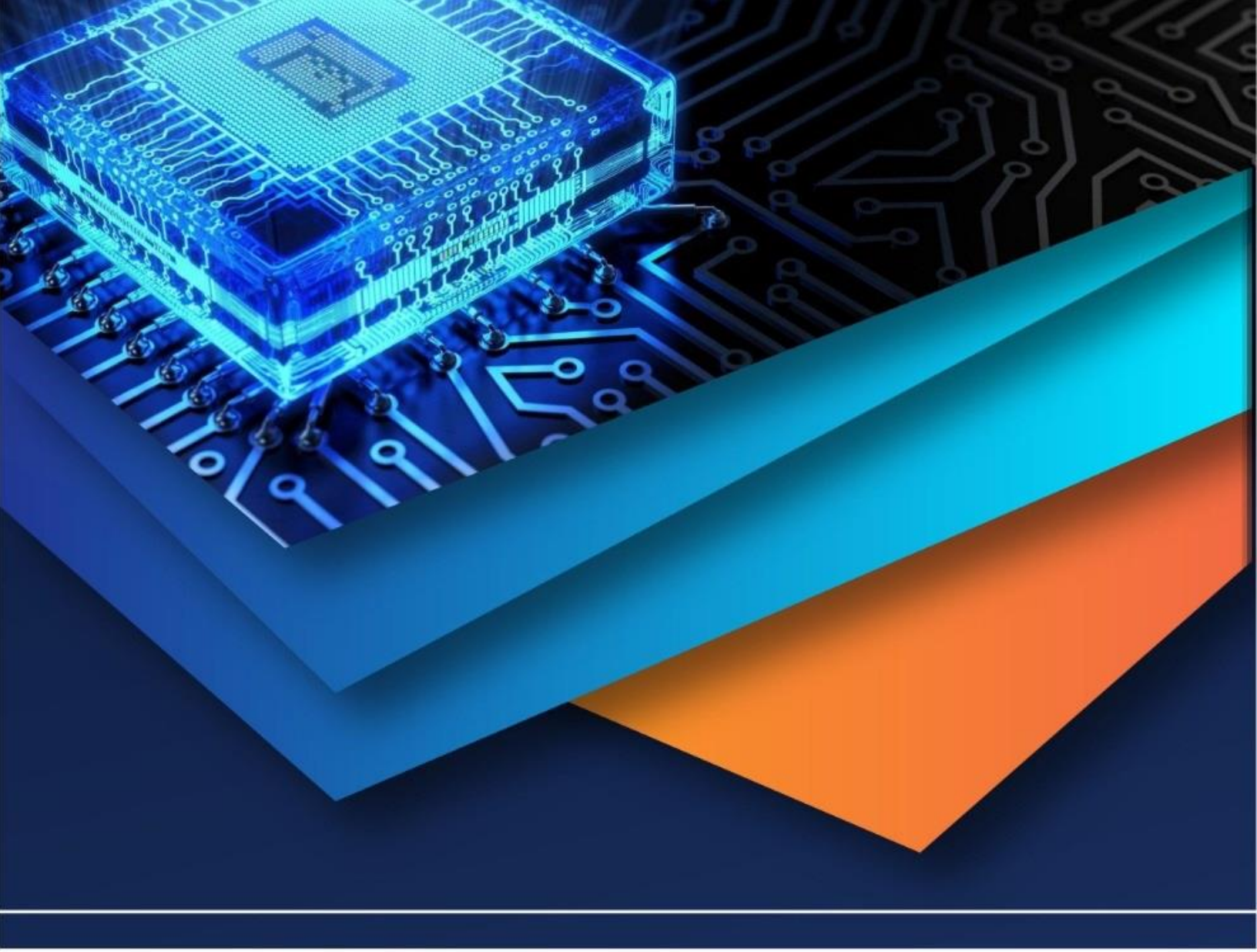
Student of M.Tech 4th Semester in Computer Science Department, Shri Shankaracharya Group of Institutions, Shri Shankaracharya Technical Campus (Approved by AICTE, New Delhi, India) Bhilai, Chhattisgarh-490020, India



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

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)