WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Digital Era and the Challenges: How to develop a positive outlook towards Digitalization

Anju Kha

Research Scholar,Department of Sociology (P.U Chd.)
Email ID: - anjukha16@gmail.com

ABSTRACT

Every day in our digital era brings with it a new invention that makes our lives simpler, but it also brings with it new difficulties and fears. The most pressing issue in the digital world is not how technology will evolve, but how it will be handled to ensure perfect security. The purpose of this article is to highlight the importance of developing a positive attitude toward digitization as well as the preventive steps that can be taken to protect ourselves from being victims of cybercrime.

Keywords: - Digital, Hacking, Cybercrime, Challenges

Introduction

India began its journey in the digital world on 15th august 1995 when VSNL (Videsh Sanchar Nigam Limited) launched the internet services.With the advent of internet, it became a medium of global collaboration, interaction and connectivity shattering the distance barrier. And with the passage of time the technological transformations in digital world keeps on shifting from network of heavy computer to laptop and now in our mobile phones which had made peoples life's easier to do all those tasks which use to take a lot of their time and efforts. Today, accessing information, selling, purchasing has become so easy that in one click we can get an abundance of information in our hands on our devices and can do all other task within a fraction of seconds.

Digital India Campaign

With an aim to build a digitally empowered knowledge economy the government of India has launched digital India campaign on 2nd July 2015. The main aim of this campaign is to improve the digital literacy of the citizens of India. It is a dream project of Indian govt which targets to improve online infrastructure, providing high speed internet facility and connecting as much as possible with the rural population to provide job-oriented schemes and government service through digital platform.

But as we are living in a digital era, every day it comes with a new innovation; making our lives easier along with this it also comes with new challenges and fear. The most important question of the digital world is not how the technology will change, but how it will be managed with complete security assurance.

Even after so many advantages of the digital platform majority of people don't prefer to use them because of the increasing number of cybercrimes. Each day we see numerous headlines of being cheated online, frauds, hacked. According to a report released by NCRB (national crime record bureau) in 2017 the cybercrimes increased by 56% as compared to the previous years. India recorded about 9500,11500 and 12000 cases of cybercrime in 2014, 2015 and 2016 respectively. One of the high-tech serious threat which is commonly faced in the online world is of Hacking. It is an unauthorized intrusion into a computer or a network. In this the hacker uses unauthorised access to or control over computer network security systems for illicit purpose.According to the 2017 Verizon Data Breach Investigations Report (DBIR), 62% of breaches feature hacking (Verizon, 2017). These statistical figures are enough to threatens the trust of the people and because of this people don't prefer or we say hesitate to use digital platforms.

So, there is a dire need to work on building up the trust of the people on these digital platforms and this can be done by making people more and more aware of the ways to protect them from being a victim of hacking.

Precautionary measures

Although a 100 % secure security system is impossible in the digital age since new forms of cybercrime emerge every day like online frauds, scams, intrusions, security breaches; the only thing individuals can do is take as many precautions as possible because each precaution we take creates a barrier for hackers, making their work more difficult. Even during pandemic time these frauds and scams increased in intensity. Some of the most basic

precautions that the general public may take include :-

- **Avoiding public Wi-Fi**

Always use your trusted secure connections when using credit/debit cards for any sort of sale or transaction, or even monitoring your own personal bank accounts. Public Wi-Fi has numerous loopholes for malware, so always make sure that such activities are done with your trusted safe connections.

- **Turn internet accessing Apps Off When You Don't Need It or Not Using It.**

Some of your phone's features can be used by hackers to obtain your information, position, or connection, so rather than leaving your GPS, Wi-Fi connection, or geo-tracking on all the time, switch them on just when you need them.

- **Download from trusted sources.**

Whenever you are downloading any app or any document always make sure that it has been downloaded from a trusted source that has established a good reputation.

- **Update your software and familiarise yourself with the new regulations.**

Make sure that the software or applications you're using are up to date on a regular basis so that you can stay connected to the most secure service versions and that you're always reading the most recent rules.

- **Make it a practice to read the permissions of apps.**

Before you install an app, read the permissions to see what data you're allowing it to access.

- **Use a password, lock code or encryption**

Make sure your passwords are at least eight characters long, with a combination of lower and upper case, a number, or a distinct character, and never use the auto-complete feature for passwords. You should also avoid using the same password for all of your login accounts. You may safeguard your sensitive information by using the encryption option on your phone. You can also configure your screen to time out after five minutes or have the device lock itself after a certain number of failed log-in attempts.

- **Install anti-virus and firewall software on your computer.**

Invest in effective antivirus and firewall software to protect your devices from viruses, malware, and hackers.

- **Make sure HTTPS is enabled.**

Always verify the URL for secure 'https' rather than 'http' before opening any mail or messages requesting login or account information.

- **Login alerts**

If possible, try to enable login alerts so that you can know that someone has login to your account.

As earlier said that a comprehensive security system is very difficult to acquire in digital world as every day it comes with a new form of crime, thus the government of India has taken efforts to safeguard its citizens through its various initiatives. Some of them are:-

- **National Cyber Security Policy, 2013**

The policy's aim is to build a secure and safer cyber environment while minimising damages via coordinated efforts of institutional structures, people, processes, and technology. It was the first formalized step which was taken by the government of India towards digital security with the Ministry of Communication and Information Technology, Department of Electronics and Information Technology's National Cyber Security Policy, 2013.

- **Cyber Swahhta Kendra' (Botnet Cleaning and Malware Analysis Centre)**

In order to tackle cyber security violations and prevent their increase, Government of India's Computer Emergency Response Team (CERT-in) in February 2017 launched 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre) a new desktop and mobile security solution for cyber security in India.The centre is operated by CERT-in under Section 70B of the Information Technology Act, 2000. The solution, which is a part of the Ministry of Electronics and Information Technology's Digital India initiative, will detect botnet infections in India and prevent further infections by notifying, enable cleaning and securing systems of end-users. It functions is to analyze BOTs/malware characteristics, provides information and enables citizens to remove BOTs/malwar and to create awareness among citizens to secure their data, computers, mobile phones and devices such as home routers.

- **National Cybercrime Reporting Portal**

The ministry of home affairs has launched national cybercrime reporting portal. the portal enables filling of all forms of cybercrime irrespective of the place where it happened.

- **Personal Data Protection Bill**

The personal data protection bill draft 2019 proposes to store personal data within India only, thus, addressing the concerns related to data storage on servers based in other countries. Furthermore, critical data cannot be sent outside without the permission of the data protection authorities. Under it, harsh punishments for any infractions are also contemplated.

Although many more initiatives have been taken by the government of India but still there is a need to improve a lot. Some of the suggestions are:

Suggestions:

- Imparting computer knowledge has already been a part of school curriculum but along with this there is a need to add data protection guidelines in the course.
- There is a pressing need to raise the number of cyber-protection cells as much as possible. Every state should establish at least one or two cyber security cells.
- Along with government initiatives, there is a need to collaborate with various non-governmental organisations (NGOs) to reach people on the ground level in order to gain a better understanding of the people's problems and the various reasons why they are hesitant to accept digital platforms that can actually make their lives easier.
- Workshops in schools, colleges, universities, and businesses should be held to educate people about various cyber security measures.
- Need to increase helpline numbers.
- There is a need for verifiable certificates which can be easily accessible for every social media or personal usage app.
- There is a need to create such apps and easy access instruction manual so that we get to know about the nearest available cyber protection cell.

Conclusion

The twenty-first century is a digital era. India will be one of the greatest users of digital technology in the coming future. And India has already started its journey in this regards which can be noted during the pandemic time the was a huge bounce in the usage of interne- based services from 40% to 100% as compared to pre lockdown period (Pandey et al, 2020). The digital platform is mend to provide best opportunities to each and every citizen. Only government measures would not enough to transform India into a digitally empowered, informed economy; it will take widespread support from all Indian citizens.

Yes, there no doubt that in this digital world it is full of new challenges yet if properly implemented it can make the best future of every citizen.

References

33 tips to avoid getting hacked. (2019, March 27). Retrieved from https://www.savethestudent.org/extra-guides/32-ways-avoid-cyber-hacked.html

Current State of Cybercrime Report 2019. (2019, April 30). Retrieved from https://currentaffairs.gktoday.in/current-state-cybercrime-report-2019-04201968376.html

Cybercrime cases double in 2017, 56% cybercrime cases for fraud motive: NCRB 2017 Report. (2019, October 25). Retrieved from https://www.medianama.com/2019/10/223-cybercrime-ncrb-2017/

Hacking Attacks, Methods, Techniques And Their Protection Measures. (n.d.). Retrieved from https://www.researchgate.net/publication/324860675_Hacking_Attacks_Methods_Techniques_And_Their_Protection_Measures

Internet in India. (2008, January 30). Retrieved from https://en.wikipedia.org/wiki/Internet_in_India

Leiner, Barry & Cerf, Vinton & Clark, David & Kahn, Robert & Kleinrock, L. & Lynch, Daniel &Postel, Jonathan & Roberts, Lawrence & Wolff, Stephen. (2009). A Brief History of the Internet. Computer Communication Review. 39. 22-31. 10.1145/1629607.1629613.

Pandey, A. (2019, October 30). Cyber Security Initiatives by the Government of India. Retrieved from https://blog.ipleaders.in/cyber-security-initiatives/

Pandey, N. De, R. & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on researchand practice. *International journal of information management*, (55). https://doi.org/10.1016/j.ijinfomgt.2020.102171

Panwar, M. (2017). Digital India: Scope and Challenges. *International Journal of Academic Research and development*, *2*(2455-4197), 412-415.

Shamim. (2016). Digital India – Scope, Impact and Challenges. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, *3*(12), 90-93.

Singh, A., & Singh, N. (2017). Digital India: To Transform India into a Digitally Empowered Society.Retrieved from https://www.researchgate.net/publication/321722968_Digital_India_To_Transform_India_into_A_Digitally_Empowered_Society

Srivastava, S. (2017). Digital India - Major Initiatives and Their Impact: A Critical Analysis. *ELK ASIA PACIFIC JOURNAL OF MARKETING AND RETAIL MANAGEMENT*, *8*(3). doi:10.16962/EAPJMRM/issn. 2349-2317/2015

Statistics- National Crime Records Bureau. (n.d.). Retrieved from http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/Crime%20Statistics%20-%202016.pdf

Steps Taken to Deal with Cyber Crime and Cyber Security. (n.d.). Retrieved from https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226

Verizon (2017). "Verizon Data Breach Investigations Report 2017" http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/