# Cyber Security Awareness: A Movement of Digital Literacy Towards making of Digital India

**Dr. Shriram D. Raut[1], Dr. Ashok R. Shinde[2] , Dr. M. K. Patil[3]**

[1]*School of Computational Sciences, P. A. Holkar Solapur University, Solapur*
**sdraut@sus.ac.in**

[2]*School of Computational Sciences, P. A. Holkar Solapur University, Solapur*
**arshinde@sus.ac.in**

[3]*Bharati Vidyapeeth AKIMSS, Solapur*
**patilmahdevk@gmail.com**

## Abstract

The Digital India mission is a transformation of routine happenings and transactions to be made in digital mode using digital platforms and media. Beside this it's a well known programme of the Indian Government with a mission so as to empower Indian societies and knowledge economy using digital media and platforms. As the transformation and revolution does not happen in just a moment of time, it requires a time to educate and literate people the trends of technology. Also followed by do's and don'ts tips in view of using digital media and platforms. While considering the Indian societies and it's in depth literacy of handling digital data and media is so limited and hence gives rise to be a victims of cyber crimes. Cyber Crimes are the forgery made using computer, networked devices that lead to committing fraud, stealing identities or violating privacy. In this regard, the Cyber Security branch which deals is a system that protects devices from digital attacks. It protects data from theft and damage. There is an immense need for cyber security awareness and it would be a great movement of Digital literacy towards making and transforming Digital India.

**Keywords:** Cyber Security, Cyber Crime, Firewall, Phishing, Impersonation

## I. Introduction

India is marching towards becoming developed nations with its overall development by initiating projects such Make in India and Digital India. Digital India is a movement of digital transformation of India in all aspects of economy and digital literacy. Digital India is an initiative launched by Indian Govt to make digitally empowered society and knowledge economy [1]. The launch of this flagship programme, a lot of trust is essential so as to

guarantee digital governance and boost the economical growth that inculcates digital services, products, manufacturing and recruitment opportunities. This project would have the entire management of the ecosystem by using Digital Technology. The Govt have been successfully placed the application programs and that too got very well appreciated by the whole world in Pandemic time. The COWIN app, Arogya Setu, UMANG under the lead of the Ministry of Electronics & Information Technology [2].

Information and communication technology stands on the basis of use of digital devices and media. The digital devices and media are to be protected from people, who are actually digital attackers to create nuisance in the way this information communication technology is to be used.

The digital attacks are to be called cyber attacks and crime resulting from such attacks is called cyber crimes [3]. The word ``Cyber '' itself stands for anything by use of or related to computers, information technology and virtual reality or simply a computer network [4]. Cyber crimes are nothing but the misuse of technology in order to commit fraud, stealing identities or violating privacy and earn some money out of it. As per National Cyber Crime Reporting Portal, cyber crimes can be reported over there and are categorized as digital transaction frauds, honey trap using social media etc [5]. Computer security threats are the attacks that cause disturbance in the functioning of computers and are viruses, trojans, phishing mail/URL, Botnet and Keylogger etc. [6].

Thus cyber security awareness is needed to not be a victim of cyber crimes. Cyber security awareness is a mission in which do’s and don'ts are suggested as safety tips and other counter software programs to protect our digital devices from cyber attacks. Cyber security awareness is an initiative of digital literacy everyone should have to boost the implementation of Digital India Programme.

## 2. Cyber Crimes And Its Type

A cybercrime is caused through the use of computers, digital devices and networks [3] [7]. This basically includes digital fraud and troublesome activity by means of stealing money from online bank accounts. Further humiliation by means of defamation of an individual on social media, sharing and forwarding unsecure hyperlinks so as to infect computer systems with viruses etc. We will see some of major cyber crimes and are as belows-

- **Identity Theft :** It is the practise of unknowingly gaining other person information without the person's consent. The information about the person may include his/her name, phone number, address, or credit/debit card number etc.
- **Obtaining access to Social Media:** A cyber criminals hack or gain access to the social media account of the person. A criminal, after gaining access to the account, then tries to misuse private information and photos. A criminals forward abuse matter on hacked profiles.
- **Credit/Debit Card Skimming :** Criminal use to do Credit or Debit card duplication using a electronic device considered as skimmer. The confidential details stored on the magnetic stripe of the card are captured through that skimmer. Cyber criminals use to hack data to make online financial transactions. Further it could be used to manipulate duplicate electronic cards and take out money from ATMs.
- **Matrimonial frauds:** Online match making of life partners have been launched in the form of matrimonial websites using which young people and their parents search, interact and choose a suitable partner. But if this is to be dealt with, using untrusted and unreliable websites may lead to matrimonial frauds.
- **Online Financial Frauds:** Internet banking seems to be in use as a user comfortable way for using digital financial transaction services such as money transfer, getting account statements, payment of fees and bills, use of digital payment gateways and wallets etc. Such user banking information could be hacked or gained through telephonic/email contacting and ilegaly accessing an account could lead to have online frauds by intruders.

## 3. Cyber Security Awareness

Cyber-attacks are happening on the internet on a per day basis. A small negligence in handling digital devices could give a chance to cyber criminals to destroy everything. According to a research study of the research organization, most of all cyberattacks are digital work force attack peoples indulgence [8]. Therefore, awareness of cyber security tips gains an attention to save common man’s money and self esteem. Cyber security awareness has a vital role in keeping mankind safe from cyber threats in the digital world.

By means of Cyber Security Awareness, a cyber digital literacy could be suggested to handle above given cyber crimes and are as belows-

- **To handle Identity theft:**Cyber Security tips suggest that the person should not shut the chrome window application without signing out of the user account. It is always advised to have in practice verification of login attempt while using other than personal digital devices. A good practice is to not to save or opt autosave for username and password in the web browser. It is useful to activate a mobile alerts in the event of unauthorized login to the social media account.
- **To handle Social Media frauds:** Cyber Security literate us to be sensitive not to accept any requests from unknown people on social media sites. Criminal mind people often open duplicate/fake social media profiles with an intention to trouble innocent people. Always keep in mind not to share private details and doing financial transactions with an strangers that converse using social media platforms. Always discuss your happenings with your family and friends. Be careful about not sharing proactive pictures with anyone on social media platforms that could be mistreated or cause blackmailing to victims.
- **To handle Credit/Debit card skimming:** The cyber security expert advises that to ensure always electronic credit and debit card swiping at market malls, petrocards are to not to be done in others person's site. Also not hand over the service man to take away the debit/credit card to do the transaction. It's a good practice to observe card duplicating machine anywhere where we swipe the electronic card, preferably at diesel pumps, malls and ATM etc.
- **To avoid Matrimonial frauds:**The Security experts advise to visit verified matrimonial websites. Try to create different and new mail id for such site registration. Be careful to do a background check of the prospective match. Keeping in mind not to share any personal information also sensitive personal photographs. A special attention is to be provided for NRI profiles as most of which may be fake.
- **Dealing with Online Financial frauds :** It is always said that not to share mobile unlocking patterns or passwords with known or unknown. Mandatorily registering primary phone number and email with bank and enabled notifications. It is good practice to keep a up transaction maximum limit for the operating banking online account. Making stronger passwords by combining letters, numbers and special characters would make difficult attackers to crack. Many times people keep the same password for all its accounts. Making use of a different password for each of every account and device. It is advised that not to save usernames and passwords in the web browser, it could be a good hint to the attacker. Avoid cliking 'logged in' and

'remember' options on browser and sites, especially on free to use computers. Its security check to be made by the concern as always to check "https" shows in the web URL while doing digital transactions. A letter "s" in the URL indicates that it is "secure" access contents.

## 4. Conclusions

Cyber Security Awareness is a time demanding concern to make a secure and safe access of the digital contents using devices and media. The awareness is part of a digital literacy programme to make people learn about the do's and don'ts to protect themselves from cyber-attacks caused by the cyber criminals. The cyber criminals observe the pattern and traffic of the network that the victim accesses to do his online tasks. And on getting hints the attacker may get access to one's digital space. Thus cyber security awareness plays a vital role to make people aware to keep them awake for their safe and secure digital presence. The Indian Government under the Home Affairs Ministry has offered the Cyber Crime Reporting web Portal as part of digital literacy and cyber security awareness and also to file a complaint against the cyber-crime.

**References**

1. Morgan S., "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," Cybercrime Magazine, 13 November 2020.
2. Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K, "Guidelines for usable cybersecurity: Past and present", The 3rd International Workshop on Cyberspace Safety and Security (CSS 2011) at The 5th International Conference on Network and System Security NSS 2011.
3. Hofstede, G., Hofstede, J.G., Minkov, M., "Cultures and Organizations: Software of the Mind", 3rd Edition, McGraw-Hill USA, 2010.
4. Maharashtra Cyber, "Cyber Security Awareness for Citizens", Vol 1, 2020.
5. Ministry of Home Affairs, "Be Careful While Using Social Media Platforms", Information Booklet.
6. Ministry of Home Affairs, "Are you looking for a life partner online?", Information Booklet.
7. Ministry of Home Affairs, "Secure online Financial services!", Information Booklet.