Research Unit
Press Information Bureau
Government of India

Safeguarding India's Digital Landscape

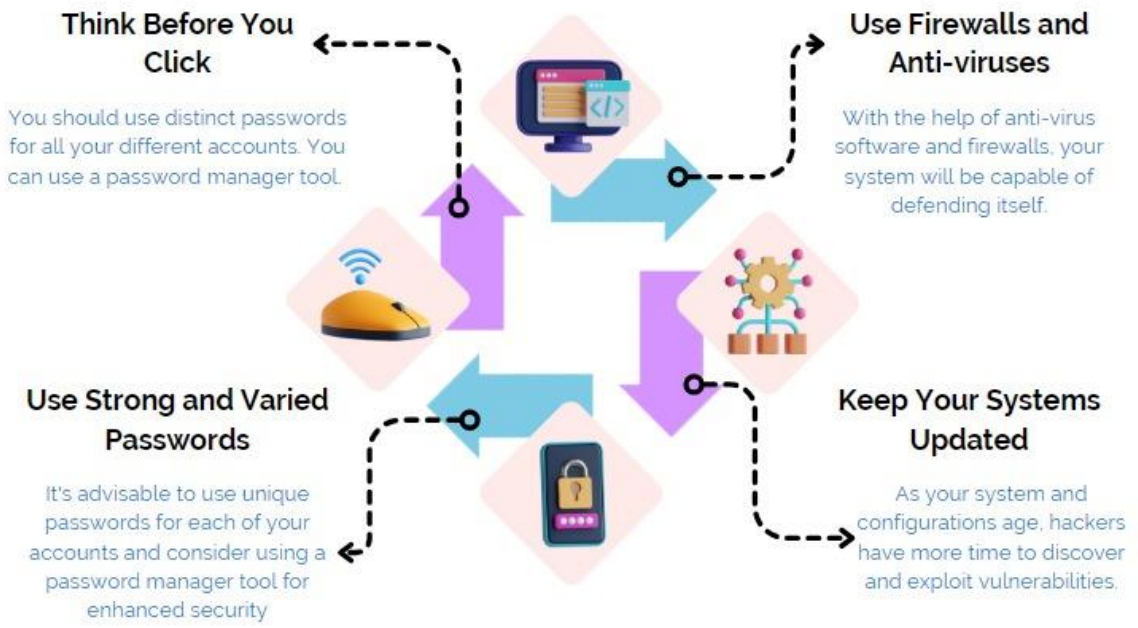
Key Government's Initiatives to Enhance Cybersecurity Awareness

July 25, 2024

Introduction

India has emerged as a global leader in the digital landscape, with a staggering 936 million Internet subscribers (Till Dec 2023, TRAI), transforming it into one of the largest connected nations worldwide. Termed as 'Digital Nagriks', Indians are increasingly integrating the internet into their daily lives, relying on it for essential needs such as business transactions, education, financial activities, and accessing government services digitally.

Recognizing the critical importance of a secure digital environment, the Government of India has been implementing robust policies aimed at safeguarding its vast online community. These measures are designed to ensure a safe, trusted, and secure cyberspace amidst the growing prevalence of cyber threats and attacks in today's interconnected world.



Understanding CERT-In

Established as the national agency for incident response under Section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) plays an imperative role in safeguarding India's cyber landscape. Operating a 24x7 incident response Help Desk, CERT-In ensures timely responses to reported cybersecurity incidents. The organization offers comprehensive Incident Prevention and Response services alongside Security Quality Management Services to enhance cybersecurity measures across the nation.

The Indian Computer Emergency Response Team (CERT-In) has registered several cases of cybercrimes during the last three years. The details are as follows.

Year	Phishing incidents	Network scanning and probing	Virus/Malware incidents	Website hacking incidents	Cyber Security incidents
2021	215	86585	9203	18	122764
2022	1145	10220	2559	57	27482
2023	401	12330	1185	39	23158

The data was provided by Minister of State Electronics & Information Technology (MoS) Jitin Prasada on 24 July 2024 in Lok Sabha.

CERT-In's efforts to combat cybercrime

CERT-In collaborates with service providers, regulators, and Law Enforcement Agencies (LEAs) to track and disable phishing websites and investigate fraudulent activities.

- CERT-In issues advisory to Ministries outlining measures to strengthen cyber security for entities handling digital personal data, including sensitive information.
- CERT-In issues advisories through RBI for audits and implementation of security practices by entities issuing prepaid payment instruments.
- CERT-In operates an automated cyber threat exchange platform for sharing tailored alerts across sectors.

- CERT-In manages the Cyber Swachhta Kendra for detecting and removing malicious programs, providing cyber security tips.
- The platform has formulated a Cyber Crisis Management Plan for countering cyber attacks across government and critical sectors.
- CERT-In conducts cybersecurity mock drills to assess readiness of organizations; 92 drills conducted with participation from diverse sectors.
- CERT-In conducts training and workshops on specialized cyber security topics and offers a self-paced Cyber Security Foundation Course in collaboration with National Institute of Securities Markets and C-DAC.

Government Initiatives to Enhance Cybersecurity Awareness

- **Cyber Crime Coordination Centre**

The Indian Government has established the Indian Cyber Crime Coordination Centre (14C) to enhance the coordinated response of law enforcement agencies (LEAs) to cybercrimes. This initiative aims to provide a cohesive framework for addressing digital threats comprehensively. Concurrently, the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) has been launched, enabling the public to report cybercrimes directly. Notably, incidents reported through this portal are automatically routed to the respective State/UT law enforcement agencies for prompt and efficient handling by legal provisions. These efforts underscore the government's commitment to bolstering cyber security and empowering citizens to contribute actively to cybercrime prevention.

- **Citizen Financial Cyber Fraud Reporting and Management System**

The Government launched the 'Citizen Financial Cyber Fraud Reporting and Management System' to facilitate the immediate reporting of financial frauds and prevent fund siphoning by fraudsters. A toll-free helpline number, '1930', has been operationalized to assist with lodging online cyber complaints, ensuring swift response and support for victims of cyber fraud.

- **Multifaceted awareness campaigns**

The Central Government has implemented a multifaceted approach to enhance the response to cybercrimes comprehensively. This includes extensive awareness campaigns aimed at educating the public and stakeholders about cyber threats, issuing regular alerts and advisories

to highlight emerging risks, conducting specialized capacity-building and training programs for law enforcement personnel, prosecutors, and judicial officers, and improving cyber forensic facilities to bolster investigative capabilities. These initiatives collectively strengthen the government's framework for addressing cybercrimes in a coordinated manner across the country.

Digital Personal Data Protection Act: Protecting citizen rights

The Digital Personal Data Protection Act, 2023 upholds individuals' rights to safeguard their personal data, incorporating established principles for data protection. These principles include obtaining consent for lawful and transparent use of personal data, limiting its use to specified purposes, minimizing data collection to necessary levels, ensuring data accuracy and timely updates, restricting storage duration to the required period, implementing robust security measures, and enforcing accountability through penalties for breaches and data adjudication.

Additionally, the Act imposes stringent protections on personal data transfers, as exemplified by the Reserve Bank of India's directive under Section 10(2) and Section 18 of the Payment and Settlement Systems Act, 2007, mandating the storage of payment system data within India. These provisions underscore the Act's commitment to robust data protection standards and restrictions on personal data transfers, which remain in effect under its framework.

Way Forward

India's digital landscape has undergone rapid expansion, with an increasingly connected population relying on digital platforms for everyday activities. Amidst this growth, ensuring robust data security measures has become paramount. The implementation of the Digital Personal Data Protection Act, 2023 reflects India's commitment to safeguarding personal data through principles such as transparency, consent, and accountability. As India continues to harness the benefits of digital transformation, maintaining stringent data protection standards will be crucial in fostering trust, resilience, and sustainable growth in its digital economy.

References:

- https://sansad.in/getFile/loksabhaquestions/annex/182/AU410_EAb9rM.pdf?source=pqals
- https://sansad.in/getFile/loksabhaquestions/annex/182/AU312_VIEADr.pdf?source=pqals
- https://sansad.in/getFile/loksabhaquestions/annex/182/AU406_kUes7H.pdf?source=pqals
- https://www.cert-in.org.in/
- https://static.pib.gov.in/WriteReadData/specificdocs/documents/2024/apr/doc2024423333101.pd

Santosh Kumar/ Sarla Meena/ Sheetal Angral/Ritu Kataria/Abhinandan Sharma