Q2 2022

Indian Cyber Crime Coordination Centre

I4C

Fifth Quarterly Issue

CYBER PRAVAHA

1st April - 30th June 2022

Government of India
Ministry of Home Affairs

CIS Division

I4C

Indian Cyber Crime Coordination Centre is as an effective apparatus to handle all issues related to cyber crime in the country. I4C acts as a nodal point in the fight against cyber crime.

DISCLAIMER

This document is for guidance and awareness purpose only. The contents of this document are not to be used for any legal validation in an investigation, judicial proceeding, etc. Utmost effort has been put into ensuring that there is no infringement of IPR. Error, if any, is deeply regretted and unintended.

Shri Ajay Kumar Bhalla
Union Home Secretary

FOREWORD

I am happy to know that the fifth quarterly issue of 'Cyber Pravaha - I4C Newsletter, Q2 2022', a publication of Indian Cyber Crime Coordination Centre (I4C) is being released. The newsletter highlights the recent developments in the field of cyber crime, and significant initiatives undertaken by I4C to support the citizens of our country, and concerned stakeholders.

2. As our cyber ecosystems expand and integrate, it is becoming more important to ensure all users can anticipate, recover and adapt quickly to cyber incidents. Law Enforcement Agencies (LEAs) shall become able to communicate the cyber risks and mitigation strategies effectively and clearly to citizens, as LEAs need to play a vital role to provide a handhold to citizens toward cyber safety. In this regard, this Newsletter provides insight into the cyber crime trends and presents analytics of cyber crime statistics.

Place: New Delhi
Date: 11.07.2022

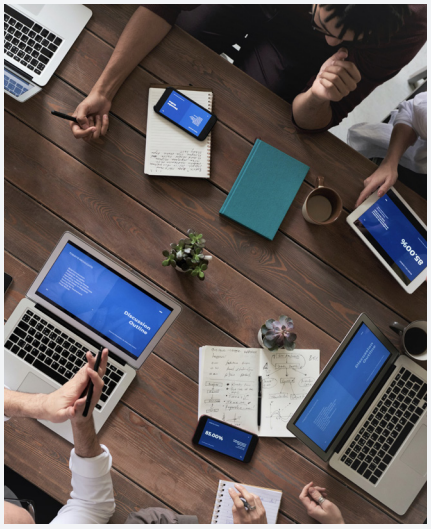
3. The digitization of our daily lives is a double-edged sword as beyond the myriad of advantages and comforts it provides, it introduces security and privacy related issues. As the stakes involved in today's data-driven world are increasing every day, hence it is required to adopt cyber resilient strategies to identify, protect, detect, respond, and recover from cyber attacks.

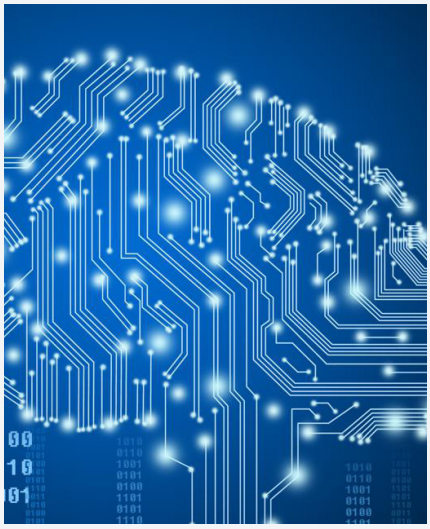
4. I compliment the team at Indian Cyber Crime Coordination Centre for undertaking this initiative of timely assessment of the ever-changing field of cyber crime, and publishing the 'Cyber Pravaha' Newsletter. As cyberspace transcends borders, we therefore need to mobilize a collective response to address systemic challenges of cyber crime. I hope this Newsletter will serve to foster collaborative approaches for building cyber resilient ecosystems.

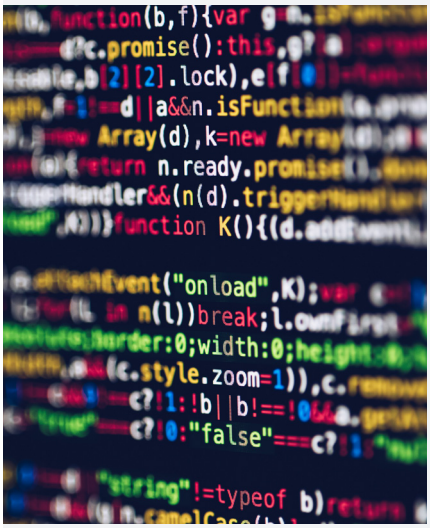
With best wishes,

(Ajay Kumar Bhalla)

CONTENTS





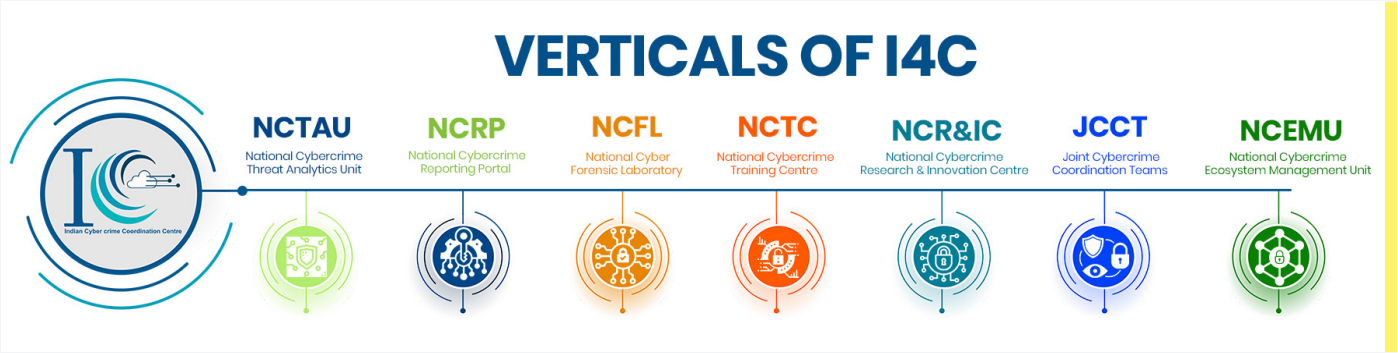


IN THIS ISSUE

ABOUT I4C

Indian Cyber Crime Coordination Centre (I4C) is an initiative of Ministry of Home Affairs, Government of India to provide a National platform for tackling cyber crime in a coordinated and comprehensive manner. I4C is working towards its vision to create an effective framework and ecosystem for prevention, detection, investigation, and prosecution of cyber crime.

I4C aims to strengthen the capabilities of Law Enforcement Agencies (LEAs) and improve coordination among various stakeholders and LEAs. It is continuously working for the enhancement of the Nation's technical capabilities to deal with cyber crime and to further strengthen the operational architecture and coordination among LEAs and other stakeholders. I4C has seven verticals: NCTAU, NCRP, NCEMU, JCCT, NCFL, NCTC and NCR&IC.

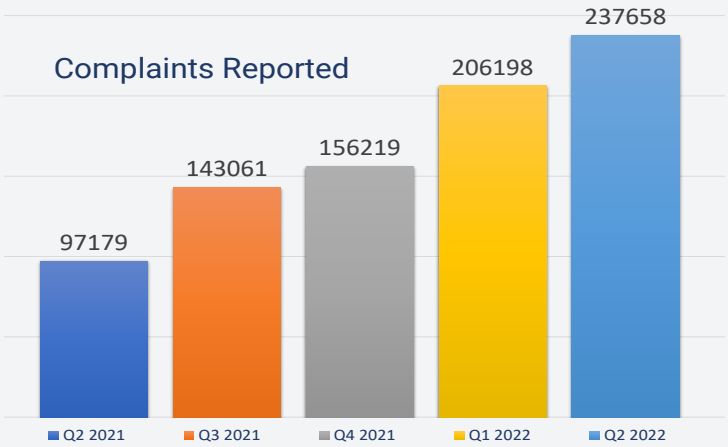


The focus of I4C has been on tackling all the issues related with cyber crime for all citizens, such as improving coordination among various Central and State agencies, driving change in India's overall capability to tackle cyber crime and facilitating capacity development of LEAs to better respond to cyber crime.

I4C also focusses on strengthening the fight against cyber crime, committed against women and children. Ease of filing cyber crime related complaints has been improved with the various initiatives of NCRP. Identification of latest cyber crime trends and patterns is also done by synergizing National Cybercrime Reporting Portal and Threat Analytics Unit of I4C.

Cyber Crime Awareness among public about preventing cyber crime has been a cornerstone in many intiative undertaken by I4C under NCEMU. I4C has assisted States/UTs in capacity building of Police Officers and Judicial Officers in the areas of cyber forensics, cyber hygiene, cyber-criminology, etc.

OVERVIEW Q2 2022



Comparative analysis of total cyber crime reported

The Newsletter 'Cyber Pravaha' covers the Second Quarter of 2022, i.e., April - June 2022. It is the fifth issue in-line with the Newsletter of Q1 2022 & Q4 2021, and the Newsletter of Q2 - Q3 2021. It provides an analysis of the cyber crime incidents reported during the period.

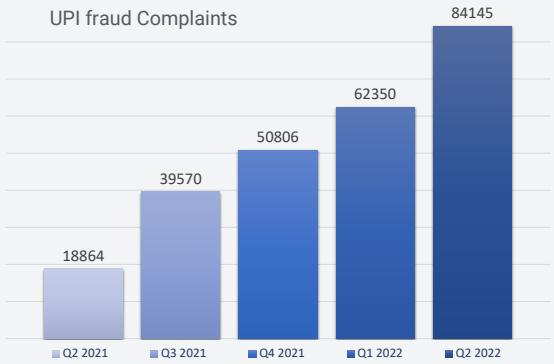
National Cybercrime Reporting Portal saw a rise of 15.3% in reported complaints during the Second Quarter of 2022 compared to the First Quarter of 2022. Total 2,37,658 complaints were reported during the Second Quarter of 2022. Technological advancements and the COVID-19 pandemic have also accelerated the reliance on digital platforms to perform daily and essential activities, making users increasingly susceptible to cyber threats.

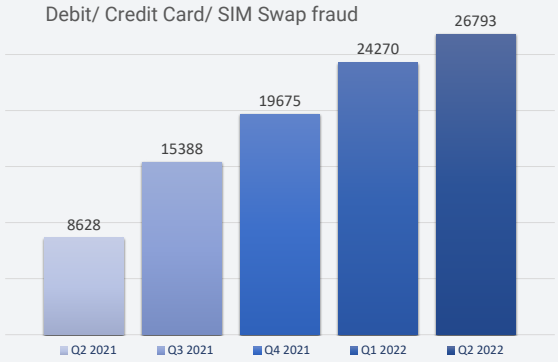
With the rise in total incidents reported, complaints under several 'cyber crime categories' have also increased considerably. Notable changes include increase in UPI Fraud complaints from 62,350 in Q1 2022 to 84,145 in Q2 2022, and increase in Debit/Credit/Sim Swap Fraud complaints from 24,270 in Q1 2022 to 26,793 in Q2 2022. Internet Banking Fraud complaints reported in Q2 2022 were 19,267.

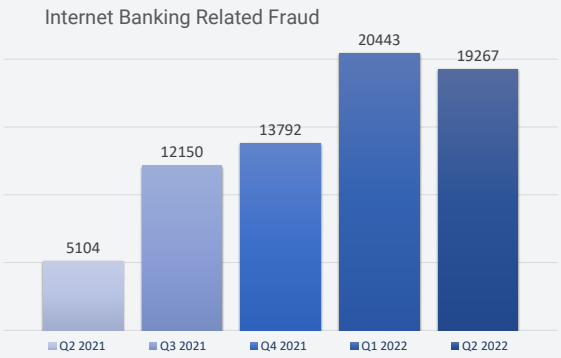
The 'Online Financial Fraud', a cyber crime category under NCRP, is the most prevalent among others, as 67.9% of the total reported cyber crime were 'Online Financial Frauds'.

National Cybercrime Threat Analytics Unit (NCTAU) of I4C has taken several steps in the field of Cyber Crime Prevention and Cyber Security Cooperation with Domestic and International Agencies through various meetings and dialogues.

All the components of I4C have made noteworthy progress in their respective fields, and the initiatives of I4C are continuing with equal zeal.







KEY STATISTICS

09 Cyber Crime Information (Advisories) shared with State/ UT LEAs and concerned stakeholders.

95 cr Rupees have been put on hold by banks under the Citizen Financial Cyber Frauds Reporting & Management System (CFCFRMS). In Q2 2022, over Rs 34 crore have been put on hold.

174 alerts were shared with stakeholders on Open Source Information Sharing System (OSISS) platform.

18,032 Police Officers from States/UTs have registered on the CyTrain Portal as of June 2022 & 5,551 Certificates have been issued after successful completion of training.

2,37,658 complaints were registered in the category of 'other crimes' on NCRP during Q2 2022.

4,953 forensic services have been provided to LEAs by NCFL as of June 2022.

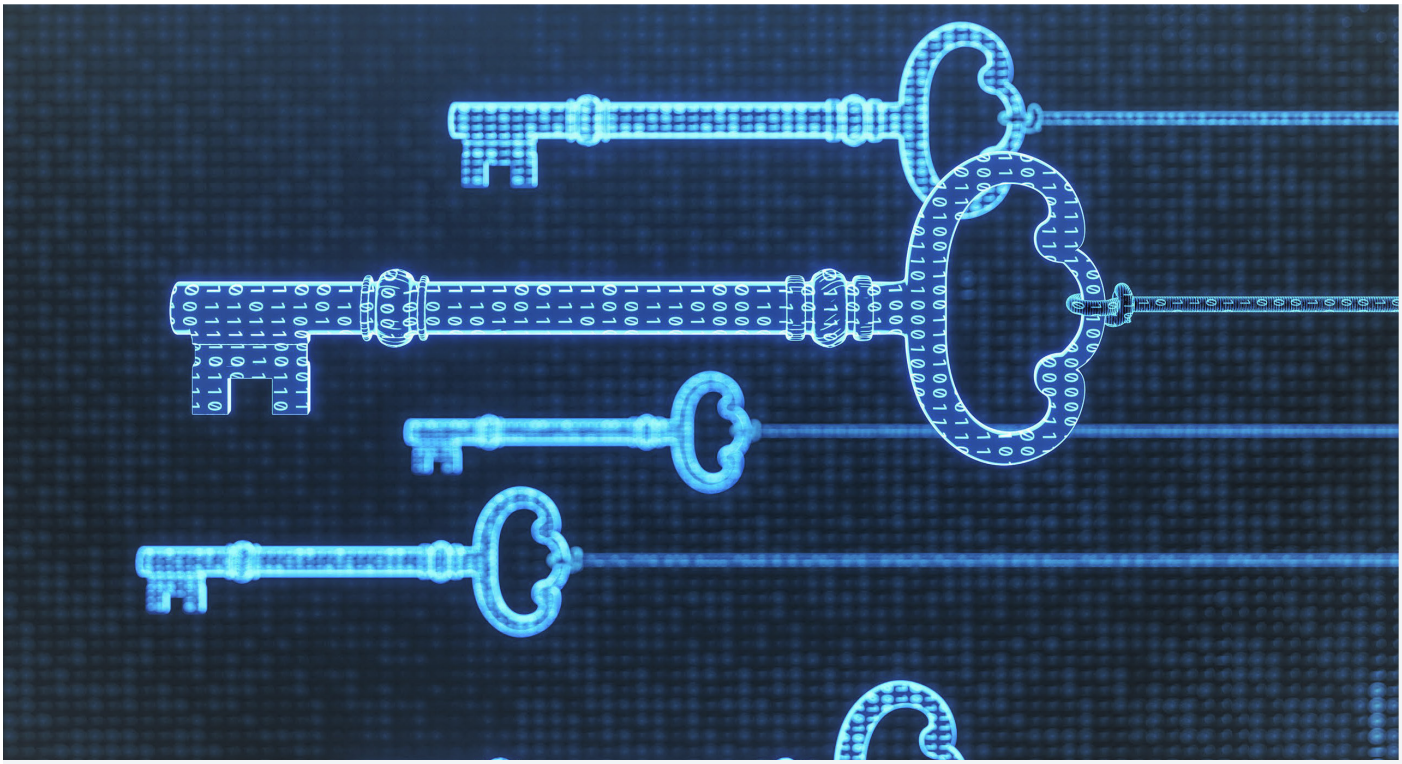
7.08 lakh details related to suspects have been collated in the Suspect Repository on NCRP

1263 tweets shared via @CyberDost, and the number of followers increased to 3.97 lakh. Cyber tips shared on various platforms such as Facebook, YouTube, Telegram, Instagram, Koo, LinkedIn, and Public.

15,587 complaints registered relating to Child Pornography/Rape Gang Rape (CP/RGR) (Anonymous) and 1,654 complaints registered related to CP/RGR (Report & Track) from April to June 2022.

12,382 inter state linkages of mobile and IMEI numbers in cyber crime cases & 22 FIRs have been shared with States/UTs under JCCT by June 2022

05 R&D projects are under process in National Cybercrime Research & Innovation Centre (NCR&IC) vertical of I4C



CFCFRMS

CITIZEN FINANCIAL CYBER FRAUDS REPORTING AND MANAGEMENT SYSTEM

CFCFRMS has been developed in house by Indian Cyber Crime Coordination Centre (I4C) to integrate Citizen reporting, Law Enforcement Agencies, Banks and other Financial Intermediaries into a single platform for effectively tackling financial cyber frauds in the country. In the Second Quarter of 2022, the CFCFRMS module has saved the amount of Rs 34.4 crore of citizens' siphoned off money by cyber fraudsters.

Since its launch in April 2021, with the help of LEAs, Banks, Wallets and other financial intermediaries this module has saved Rs.95.7 crore till June, 2022. More than 86 financial intermediaries and State/UT LEAs are working round the clock to keep citizens' hard-earned money safe and provide immediate response in cases of financial cyber frauds.

All the States and Union Territories in the country have established 1930 support centres in the respective State/UT for smooth reporting of financial cyber fraud complaints. A quick complaint from the citizen's side on 1930 helps in prompt redressal of the complaint, and minimizing the financial cyber frauds in the country.

Get in touch - i4c.finmod@mha.gov.in

95 Cr rupees saved till June 2022 under the CFCFRMS initiative of I4C, MHA

IN CASE OF FINANCIAL CYBER FRAUD IMMEDIATELY CALL 1930

WORKING FLOW OF CFCFRMS MODULE – NATIONAL HELPLINE NUMBER 1930

STEP 01/	STEP 02/	STEP 03/	STEP 04/	STEP 05/
Victim calls on 1930 to report financial cyber fraud	Police Operator submits the details provided by victim	Complaints is escalated to related banks, wallets, etc.	SMS sent to victim with Ack. number & further directions	Bank marks the defrauded money on lien (Put on hold)

KEY STEPS TAKEN

POLICY MATTERS TAKEN UP WITH RBI

I4C has taken up certain crucial policy matters for prevention of cyber crime with Reserve Bank of India (RBI) such as Re-KYC in hotspots of cyber crime, strict third party KYC, guidelines for Fintech companies, Geo location capturing during transactions, etc.

CYBER JAAGROOKTA (AWARENESS) DIWAS

All the Central/State Ministries have been requested to observe Cyber Jaagrookta (Awareness) Diwas on the first Wednesday of every month in all the Schools/Colleges/Universities/Panchayati Raj Institutions (PRIs) and Municipalities.

INTEGRATION OF PLATFORMS

The initiative to integrate the existing State/UT platforms with the existing National platforms for better use of the platforms and effectively handling cyber crime in a holistic manner.

MASS AWARENESS PROGRAM

Mass awareness program through multiple media. Publicity material and topics related to awareness suggested for imparting training by Institutions/ Academies.

IMPROVEMENTS IN CYBER TIPLINE REPORTING SYSTEM

Improvements in the system of Reporting and Retention of Cyber Tipline Reports received from the National Centre for Missing & Exploited Children (NCMEC), USA in National Cybercrime Police Portal (NCPP).

CAPACITY BUILDING PROGRAMS FOR STATE/UT LEAs

Capacity building programs for State/UT LEAs on National Cybercrime Police Portal with hands-on training sessions.

CYBER PRAVAHA – I4C NEWSLETTER & ADVISORIES 2021 BOOKLET

'Cyber Pravaha' (October 2021 – March 2022) was published in May 2022 to create awareness regarding the recent developments in the field of cyber crime. Cyber Crime Advisories 2021 booklet, consisting of all the Advisories published by I4C in 2021, shared with all the stakeholders.

CYBER SECURITY AWARENESS QUIZ

NCR&IC organised cyber security awareness Quiz for LEAs version 2.0 in April 2022. More than 2300 Police officers participated in the Quiz.

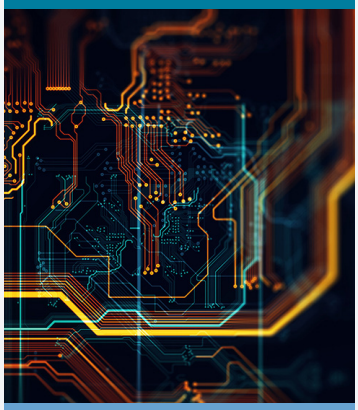
WEBINAR ON CYBER CRIME AWARENESS & CYBER SECURITY

Webinar on various topics such as 'Cloud Security Challenges and Investigation' organised by NCR&IC. Two Books related to the proceedings of Webinars namely 'Cyber Security Preparedness for next 10 years' and 'Prevention and Investigation on Phishing Crimes' released by the Union Home Secretary.

ANALYSIS REPORTS

Analysis Reports related to various cyber crime shared with concerned Division of MHA, concerned Organisations, CAPFs, State LEAs, etc.

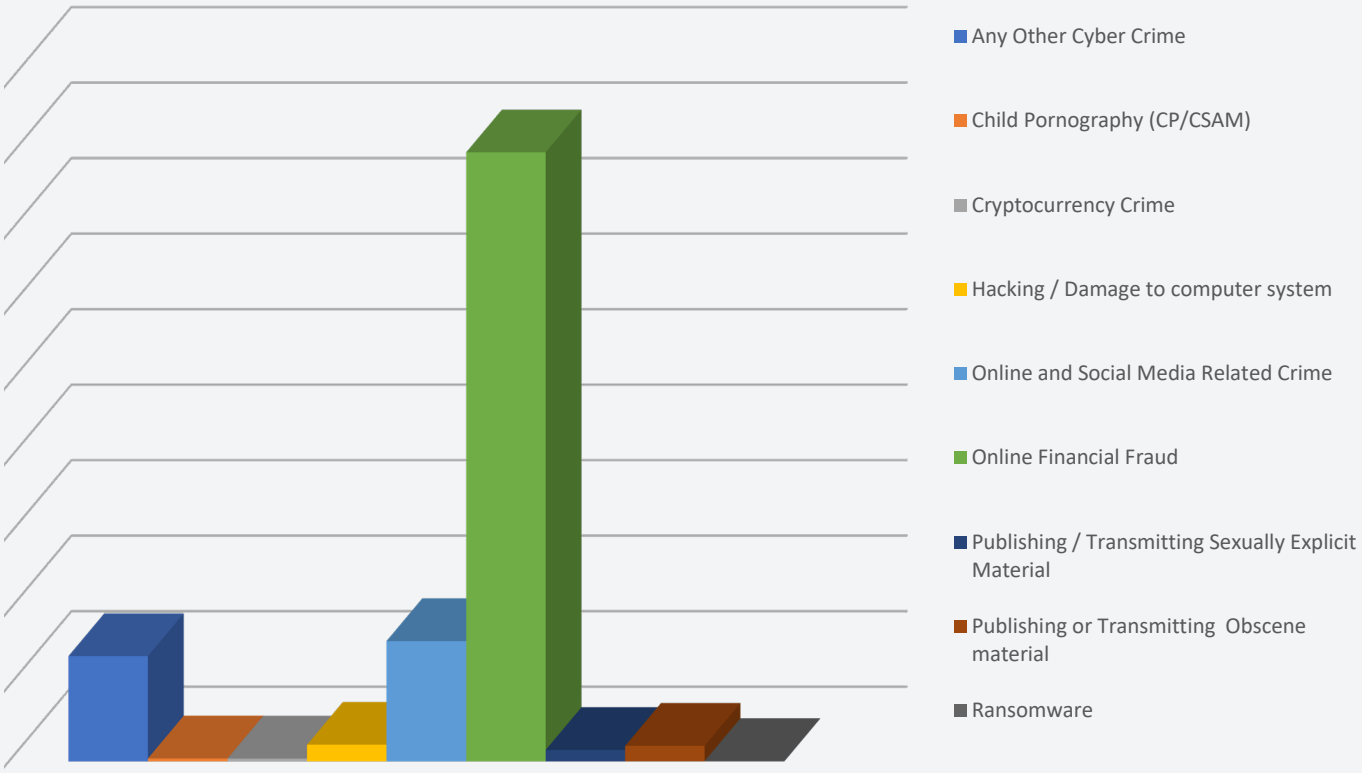
I4C engaged with various intermediaries in relation to prevent misuse of the available platforms and services by cyber fraudsters



I4C conducted a series of four sessions on 'Financial Safety in Digital Space' in collaboration with Ministry of Education (NCERT) in June 2022

CYBER CRIME REPORTING IN Q2 2022

Cyber Crime Incidents reported on NCRP from April to June 2022



PUTTING DATA IN PERSPECTIVE

Total cyber crime complaints reported in Quarter 02, 2022
2,37,658

Total cyber crime complaints reported in Quarter 01, 2022
2,06,198

TOP 3 CYBER CRIMES AFFECTING CITIZENS

Online Financial Frauds **67.8%**
Online and Social Media related Crimes **13.4%**
Any Other Cyber Crime **12.1%**

NCMEC TIPLINE SHARED WITH STATE/UT LEAs

During Q2 2022, **6,32,481** tiplines shared

15.3% increase in cyber crime complaints reported in Q2 2022.

Integration of the CCTNS platform with NCRP is under process

Analysis Reports, IOCs & Advisories shared with States/ UTs on trending cyber crimes.

A Mobile App is being developed for National Cyber Crime Reporting Portal (NCRP) for ease of reporting for citizens.

NCMEC
National Center for Missing & Exploited Children.

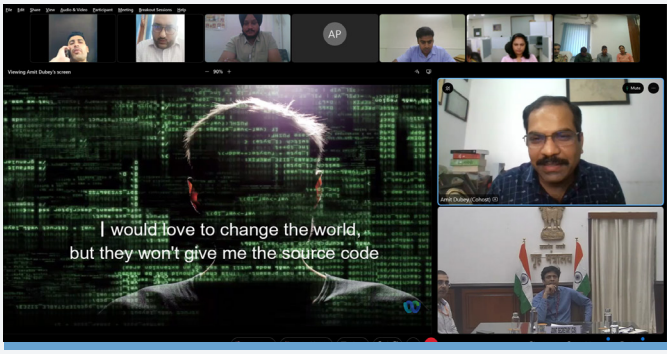
IMPORTANT EVENTS

TECHNICAL WORKSHOP FOR LEAs

FOR LAW ENFORCEMENT AGENCIES OF ALL STATES/UTs FOR EFFECTIVELY TACKLING CYBER CRIME

I4C organises monthly series of Technical workshops on Emerging Technologies used in the field of Cyber Crime.

The Online Workshop on 'Darkweb Crimes: An investigative approach' started with the brief introduction to the topic. Speakers made their Presentations before Law Enforcement Personnel from all over the country to increase their understanding on the subject, and help them effectively use the enhanced knowledge in further investigations of cyber crime cases. More than 400 Police Officers participated in the workshops.



ONE DAY WORKSHOP FOR SENIOR OFFICIALS FROM LEAs WITH IIPA

WORKSHOP ON 'MEASURES FOR DEVELOPING OF CYBER ECOSYSTEM AND PREVENTION OF CYBER CRIME IN INDIA'

One Day Workshop on 'Measures for Developing of Cyber Ecosystem and Prevention of Cyber Crime in India' was organised on 11th April, 2022 under the chairmanship of Shri V S K Kaumudi, Special Secretary (IS), Ministry of Home Affairs at Indian Institute of Public Administration (IIPA), New Delhi.

Senior Officials from State/UT Law Enforcement Agencies discussed their recommendations regarding Cyber Ecosystem and presented practically implementable solutions for Prevention of Cyber Crime in the Country. The participants also deliberated about various cyber crime threats and challenges in future on account of evolving technologies.

JOINT CYBERCRIME COORDINATION TEAMS (JCCT) MEETING

JCCT MEETING-CUM-INTERACTION OF MEMBERS CONVENED IN CHANDIGARH ON THE 2ND OF MAY 2022

The 3rd Meeting cum Interaction of JCCT was held on 2nd May 2022 in Chandigarh under the chairmanship of Hon'ble Governor of Punjab and Administrator of Chandigarh, to discuss the issues related to cyber crime and future plans.

In the meeting, the emphasis was laid upon the various cyber crime hotspots in India such as Jamtara, Mewat, Delhi NCR, West Bengal etc. Importance of separate cyber crime Police Stations, Cyber Courts, and Cyber Prosecutors was also discussed. Representatives from Financial institutions, and other stakeholders deliberated upon various prominent issues. The Public Prosecutors & Cyber Law Experts also gave insights on legal issues pertaining to cyber crime.

NATIONAL CONFERENCE ON CYBER SAFETY AND NATIONAL SECURITY

CYBER CRIME SE AZADI AZADI KA AMRIT MAHOTSAV

The Hon'ble Union Minister for Home and Cooperation, Shri Amit Shah addressed the National Conference on Cyber Safety and National Security (Azadi from Cyber Crime – Azadi ka Amrit Mahotsav) in New Delhi on 20th June 2022. The Union Home Secretary and Senior Officials from the Ministry of Home Affairs, Ministry of Culture, and other Ministries of Government of India, DGP/CPs of States/UTs were also present.

I4C, MHA in collaboration with Ministry of Culture organized various functions across the country for Cyber Safety and National Security and to propagate Cyber Hygiene, as initiatives leading to prevent cyber crime. One-day functions at seven places across the country and one central function at Vigyan Bhawan, New Delhi for Cyber Hygiene and Prevention of Cyber Crime under the banner "Azadi Ka Amrit Mahotsav" was organized on 20 June 2022.

Seven important technical sessions were held on Prevention of Cyber Crime and Promotion of Cyber Hygiene by National Cyber Security Coordinator (NCSC), Reserve Bank of India (RBI), Indian Computer Emergency Response Team (CERT-In), Department of Telecommunications (DoT), National Payments Corporation of India (NPCI), and National Critical Information Infrastructure Protection centre (NCIIPC).

The Union Minister for Home and Cooperation, Shri Amit Shah addressing the National Conference on Cyber Safety and National Security on the 20th June 2022 at Vigyan Bhawan, New Delhi

INITIATIVES OF STATES/UTs

I. CYBER APRADH SE AZADI

07 STATES/UT ORGANISED CYBER HYGIENE AND CYBER AWARENESS RELATED FUNCTION IN JUNE 2022

As part of the 'Azadi Ka Amrit Mahotsav' celebrations, I4C, MHA in coordination with Ministry of Culture, State/UT Police of Uttar Pradesh, Assam, Gujarat, Telangana, Chandigarh, Andhra Pradesh, and Jharkhand organised various functions at 75 different places on Cyber Hygiene and Awareness for Prevention of Cyber Crime. The initiative was undertaken from 8th June 2022 to 17 June 2022, to create mass awareness among citizens against increasing cyber crimes and to propagate National Helpline Number 1930 for responding.

The significant aspects of the program were participation at Police Station level, inclusion of National School of Drama (NSD) for creating cyber awareness through Nukkad Nataks, various academic institutions, participation of students from educational institutions, etc.

II. CAPACITY BUILDING PROGRAMS FOR STATE/UT LEAs

TECHNICAL SESSIONS FOR LAW ENFORCEMENT PERSONNEL FOR EFFECTIVELY TACKLING CYBER CRIME

Ladakh Police: A technical session on the aspects of cyber crime was organised in coordination with Ladakh Police in May 2022 in Leh. Cyber Awareness for prevention of Cyber Crime was at the focus of the session. Technical experts from Indian Cyber Crime Coodination Centre also conducted a query session for Ladakh Police officials.

Assam Police: Frequent alerts through official social media pages of respective districts, CID (Assam) & APHQ were posted for alerting the public about fraudulent practices adopted by Cyber crimnals. Distribution of leaflets, placing banners/posters to increase awareness.

III. CYBER TRAINING WORKSHOP BY UTTAR PRADESH POLICE

To impart technical knowledge to the Police force which will be deployed at the newly formed Cyber Crime Helpdesk at all the Police Stations across the State, Uttar Pradesh Police conducted an online cyber training workshop on 27th June 2022.

IV. NEW CYBER CRIME POLICE STATIONS IN HARYANA SANCTIONED

The Haryana Home Department sanctioned 29 new Cyber Crime Police Stations for the State, of which three have been set up in Gurgaon to handle a surge in cyber crime cases.The new cyber crime Police Stations will also run awareness programmes for common people and students regularly in-person and also by running social media campaigns.

V. MEG-COPWATCH - WOMEN SAFETY BY MEGHALAYA POLICE

CID, Meghalaya Police has also taken the initiative of launching the Meg-Cop Watch Application, which is a mobile application that seeks to provide safety and security to women and children in distress.

INITIATIVES OF STATES/UTs

VI. ANDHRA PRADESH POLICE

03 Cyber Crime Police Stations established in Andhra Pradesh

01/ Bank put on hold under CFCFRMS (1930) in Andhra Pradesh in Q2 2022

1.97 Crore

02/ Andhra Pradesh Police conducted various Cyber Awareness programmes among the citizens to aware them regarding the latest modus operandi of cyber crimes

03/ Several capacity building Workshops were organised on 'Cyber Crime Investigation' for Station Officers and Investigation Officers

04/ Wide publicity of Financial Cyber Crime Helpline number '1930' and 'National Cybercrime Reporting Portal' i.e. www.cybercrime.gov.in was given

05/ As part of the 'Azadi Ka Amrit Mahotsav' celebrations, Andhra Pradesh Police, in coordination with Ministry of Home Affairs and Ministry of Culture, organised various functions at different places on Cyber Hygiene and Awareness for Prevention of Cyber Crime. Police Station level, Programs held at various places in the State on 14th June 2022

06/ Seminars and various other programs related to awareness on cyber offences conducted with the students in Degree Colleges and Engineering Colleges

07/ A Cyber Laboratory has been established in Guntur District for analysis of Cyber Crimes

Cyber Awareness Programs by Andhra Pradesh Police in various Educational Institutions

INITIATIVES OF STATES/UTs

VII. KERALA POLICE

20 Cyber Crime Police Stations have been established in all Police districts of Kerala

01/ Bank put on hold under CFCFRMS (with National Helpline No 1930) in Kerala in Q2 2022

72.3 Lakhs

02/ Kerala Police, CCSE Centre frequently conducts Operations to trace those involved in circulating CSAM online

03/ Awareness created among public, especially students, various seminars and meetings conducted in Schools, Colleges, Resident Association Halls, Office premises of Cyber Police Stations in all districts

04/ BSafe of Cyber Dome introduced new features to its platform such as BScan, BSafe talks, Cyber Safety Awareness Handbooks and other BSafe resources

05/ Webinar on understanding Cryptocurrency Scams and current regulations for citizens

Training of Law Enforcement officials on investigation techniques to combat online child sex abuse.

INTERNATIONAL COOPERATION

SECOND SESSION OF THE AD HOC COMMITTEE (AHC)

Ad Hoc Committee to elaborate a comprehensive International Convention on Countering the Use of Information and Communications Technologies (ICTs) for criminal purposes, established by the UN General Assembly in its resolution 74/247, held its second session in Vienna, 30 May to 10 June 2022.

EIGHTH MEETING OF THE BRICS WORKING GROUP

The 8th meeting of the BRICS Working Group was held in May 2022 regarding Security in the use of Information and Communication Technology (ICT) in virtual mode.

SIXTH INDIA – GERMANY BILATERAL CYBER DIALOGUE

The 6th India-Germany Bilateral Cyber Dialogue was held in April 2022 in Bonn and Berlin, Germany. Discussions on the latest developments in the national cyber policies and strategies in the areas of cybersecurity were held.

FIFTH INDIA – UK BILATERAL CYBER DIALOGUE

India and the UK held their Annual Cyber Dialogue in London in April 2022. Both sides welcomed the substantial bilateral engagement which covered cyber governance, deterrence and mutual resilience. They reiterated their commitment to a joint programme of action and next steps in implementing the Enhanced Cyber Security Partnership.

FOURTH INDIA – JAPAN CYBER DIALOGUE

The Fourth India-Japan Cyber Dialogue was hosted by India virtually on 30 June 2022. Both sides discussed important areas of bilateral cyber cooperation and reviewed the progress achieved in the areas of cybersecurity and Information and Communication Technologies (ICTs) including 5G Technology.

COUNTER RANSOMWARE INITIATIVE (CRI)

The CRI Second Resilience Working Group meet was held in May 2022 to discuss methodologies to counter ransomware, important ransomware incidents and experiences for predictive analysis, Governments' involvement and role in managing ransomware incident response, and how to incentivize reporting of ransomware incidents among other related issues. India participated as a lead in the Resilience working group meet.

India and the United Kingdom reaffirmed the commitment to an open, secure, stable, accessible and peaceful cyberspace, which can be enjoyed by all with India-UK Cyber Statement, April 2022

First ASEAN Regional Forum (ARF) Workshop on Terminology in the Field of Security of and in the Use of ICTs in April 2022

CYBER UPDATE

CERT-IN DIRECTION ISSUED IN APRIL 2022

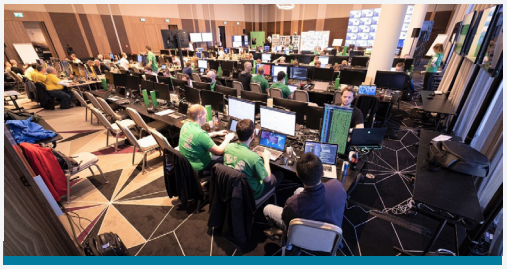
On 28th April 2022, CERT-In issued a direction under Section 70B(6) of IT Act. The Direction has significantly widened the types of cyber security incidents that must be mandatorily reported to CERT-In. A strict timeline of 6 hours after notice of the incident has been established for reporting such incidents to CERT-In. The directions also cover aspects relating to synchronization of ICT system clocks, maintenance of logs of ICT systems, etc.

NATIONAL CYBER EXERCISE – NCX INDIA

National Security Council Secretariat (NSCS) organised National Cyber Exercise (NCX) India, which was conducted from 18th to 29th April 2022 with the aim to train Senior Management and Technical personnel of Government/Critical Sector organisations on contemporary cyber threats and handling cyber incidents and response - to strengthen India's Cyber posture.

BUREAU OF CYBERSPACE & DIGITAL POLICY – CDP

The US Department of State established the Bureau of Cyberspace and Digital Policy (CDP) in April 2022 to address the national security challenges, economic opportunities, and implications for U.S. values associated with cyberspace, digital technologies, and digital policy. The CDP Bureau includes three policy units: International Cyberspace Security, International Information and Communications Policy, and Digital Freedom.



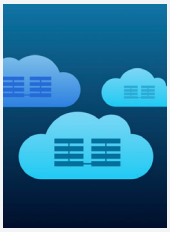
CYBER DEFENCE EXERCISE LOCKED SHIELDS 2022

Locked Shields is one of the largest and most complex international live-fire cyber defence exercise, organised annually by CCDCOE since 2010, which enables cyber security experts to enhance their skills in defending National IT systems and critical infrastructure under real-time attacks. The team from Finland won the Locked Shields 2022.

INTERNATIONAL PROTOCOL FOR SHARING E-EVIDENCE

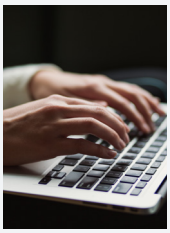
The 2nd Additional Protocol to the Convention on Cybercrime (Budapest Convention) on enhanced co-operation and disclosure of electronic evidence provides a legal basis for disclosure various e-evidence, mutual assistance tools, as well as personal data protection safeguards. By June 2022, 24 Countries have signed the protocol.

CYBER GLOSSARY



CLOUD

Servers that are accessed over the Internet, and the software and databases that run on those servers, instead of hosted locally



SPEAR PHISHING

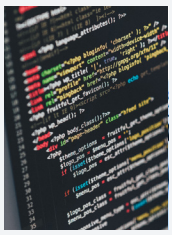
A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts

RANSOMWARE

Malicious software that makes data or systems unusable until the victim makes a payment

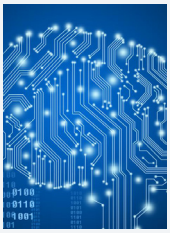
WHITELISTING

Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications



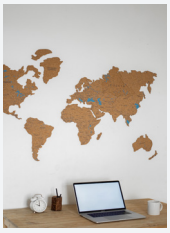
BOTNET

A network of infected devices, connected to the Internet, used to commit co-ordinated cyber-attacks without their owners' knowledge



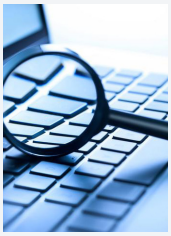
WHALING

Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.



INTERNET OF THINGS (IoT)

Devices with software that connect and exchange data with other devices and systems over the Internet

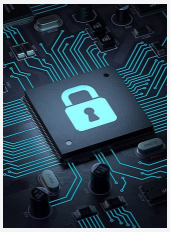


PATCHING

Applying updates to firmware or software to improve security and/or enhance functionality

SOCIAL ENGINEERING

Manipulating people into carrying out specific actions, or divulging information, that's of use to a cybercriminal



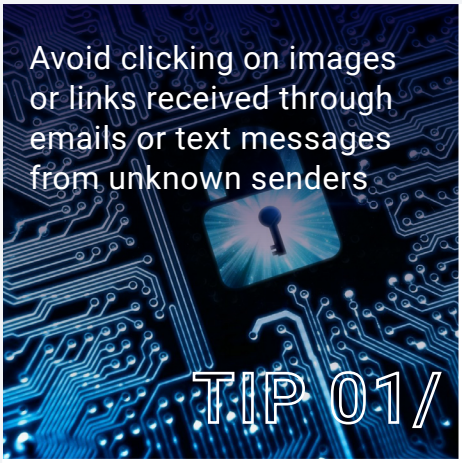
ENCRYPTION

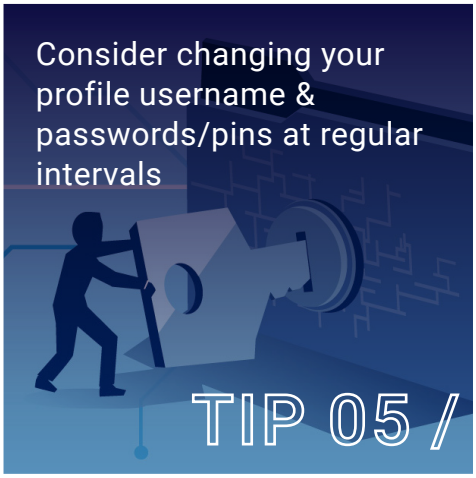
Securing digital data using one or more mathematical techniques, along with a password or key used to decrypt the information

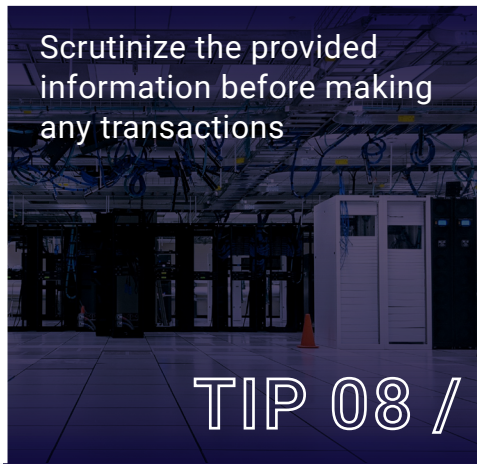
CYBER HYGIENE TIPS

An increasing number of individuals and organisations are being seriously impacted by cyber incidents. Hence, maintaining Cyber Hygiene is critical to prevent such incidents.

End users' cyber hygiene practices often play a large role in cyber incidents. It is essential that each and every official of an organisation develops a deeper understanding of the good cyber hygiene practices, and update themselves with changing scenario of the cyber world. They also need to protect their personal information and maintain organisations' information security.







Indian Cyber Crime Coordination Centre

CYBER PRAVAHA

Q2 2022

Prepared by NCTAU - National Cybercrime Threat Analytics Unit, I4C

Contact us Tel: 011-23438207 | Address: NDCC II Building, Jai Singh Road, New Delhi


@cyberdosti4c


@CyberDosti4c


@cyberdosti4c


@cyberdost


@cyberdosti4c


@cyberdost.i4c


@cyberdosti4c


@cyberdost


@cyberdost