Annexure – I
WRITE UP

Government of India
Ministry of Home Affairs
Indian Cyber Crime Coordination Centre (I4C)
(CIS Division)
***

Sub: -Commencement of 'CyberJaagrooktaDiwas' on First Wednesday of every month commencing from 6thOctober, 2021 (Wednesday)

Introduction

1. Cyber space is a complex and dynamic environment of interactions among people, software and services supported by world-wide distribution of Information and Communication Technology (ICT) devices and networks. On the one hand, cyber space, which cuts across global boundaries has brought in latest innovative technologies and modern gadgets, while on the other hand, it has inevitably led to increased dependencies on computer resources and internet-based professional, business and social networking.

2. The exponential increase in the number of internet users in Indiaand the rapidly evolving technologies have also brought in its own unique challenges, besides aggravating the existing problems of cybercrimes, which is one of the fastest growing forms of transnational and insidious crimes.

3. These technological developments have also led to the proliferation of cybercrimes, which is one of the fastest growing forms of transnational and invisible crimes. The borderless nature of cybercrimes poses challenges in responding effectively due to the limits of cross-border investigation, legal and jurisdictional challenges and diversity in the technological capabilities to combat this virtual crime space spread across the globe.

4. Cybercrimesare generally understood as malware attack (use of malicious software like ransom ware, viruses, trojans, spyware, bots etc.), phishing (capturing sensitive information like username, password, credit/debit card details using fake websites, emails etc.), attacks on critical infrastructure, unauthorized data access (data breach), online financial frauds, crimes against women and children like cyber stalking, child pornography etc.

5. There is a need to increase 'cyber hygiene' for prevention of cyber crimes by inculcating habits of taking basic care of ICT devices at regular intervals, such as, properly shutting down the computer, changing passwords at regular intervals, being cautious against opening of phishing websites along with other websites, precautions to be taken while handling social media platforms, protection against data theft,collection and disposable of E-waste etc.

6. Further, continuous efforts are required on frequent basis to remind the citizens about the cardinal principles of cyber hygiene to ensure safety against cyber