

**F. No. 5-6/2021-PN-II
Government of India
Ministry of Education
Department of Higher Education
(PN.II Section)**


**Shastri Bhawan,
Dated : 8rd February, 2021**

OFFICE MEMORANDUM

Subject: Letter from Ministry of Home Affairs regarding curbing cybercrimes and develop an ecosystem for cyber security in Indian educational institutions cyber space– reg.

The undersigned is directed to forward herewith a copy of letter dated 25.01.2021 from Deputy Secretary (I4C), Ministry of Home Affairs regarding curbing cybercrimes and develop an ecosystem for cyber security in Indian educational institutions cyber space, which is self-explanatory.

2. It is requested that the content of the letter may be circulated among Universities/Centrally Funded Technical Institutions/Colleges etc under your administrative control for wide publicity and necessary action may be taken in the matter.


(D. T. Pali)

Under Secretary (PN-II)

All Bureau Heads of D/o Higher Education

Chairman, UGC

Chairman, AICTE

819791

No: 22003/05/2019-CIS-II
Government of India
Ministry of Home Affairs
(Indian Cyber Crime Coordination Centre)

5th floor, NDCC-II Building, New Delhi
Dated, the 25th January, 2021

To,

1. Shri Rakesh Ranjan,
Additional Secretary (for
IITs, IIITs, TE, TC,
IISERs, IISc, etc.)

2. Dr. Vineet Joshi,
Additional Secretary (for
Central Universities,
NER)

3. Smt. Kamini Chauhan
Ratan, Joint Secretary,
Higher Education, (for
UGC, NEP)

4. Shri Sanjay Kumar
Sinha, Joint Secretary,
Management &
Language, (for
Management and IIMs)

Sub: Curbing cybercrimes and develop an ecosystem for cyber security in Indian educational institutions cyber space - reg.

Sir/Madam,

The Ministry of Home Affairs (MHA) has setup the Indian Cyber Crime Coordination Centre (I4C) to strengthen the capability of prevention, detection, investigation and prosecution of cybercrimes, in a coordinated and comprehensive manner. Further, MHA on 30.08.2019 has operationalized the National Cybercrime reporting Portal, which provides for a centralized mechanism of complaint reporting by citizens relating to cybercrime. There is a special focus in the portal on cybercrimes against women and children and it allows the de-centralized dealing of each complaint by the Law Enforcement Agencies (LEAs) of the State/UT concerned.

2. The I4C is actively involved in developing a robust ecosystem for securing the cyber space, giving due emphasis on capacity building and public awareness etc. During an interaction on 22.10.2020 held with the various academias, viz. Delhi University, IIT Delhi, AICTE, IIIT Delhi etc and the representatives of UGC, it was felt that there is a need for a multipronged strategy to tackle the unforeseen challenges of cybercrime.

3. With a view to strengthen the cyber security and to give impetus to the capacity building efforts, I am directed to request you to take up the following issues with the concerned agencies:

i. To kindly consider giving wide publicity to the MHA twitter handle @CyberDost, which provides updates and advisories at regular intervals for prevention of cybercrimes.

DS(UGC)
DS(NEP) (1)

2/1/2021
UC(PN-IT)

Secy MHA
6/1/21

Sh. HK
2/1/21

- ii. To kindly consider giving wide publicity to the 'National Cyber Crime Reporting Portal' i.e. <https://cybercrime.gov.in> in all Universities and Colleges in the country and provide link of the 'National Cyber Crime Reporting Portal' i.e. <https://cybercrime.gov.in> on the websites of autonomous bodies, attached offices, subordinate offices, etc under M/o Education.
- iii. A "Handbook on Cyber Hygiene" may kindly be prepared in vernacular languages on cyber security, prevention of cybercrime etc. for the students of all Universities and Colleges in the country.
- iv. A common "Cyber Safe" Curriculum may kindly be designed with emphasis on 'Hands-on-Training' at Graduate/ Postgraduate level in all streams (i.e. Engineering/ Science/ Commerce/ Management/ Arts/ Medical/ Business Administration etc) which may be taught in all Colleges and Universities and build cyber safe environment in the country. The suggestive list of topics to be covered in various streams is enclosed herewith.
- v. A "Baseline Policy" may kindly be formulated with Do's and Don'ts in cyber security for all Universities and Colleges.
- vi. Regular competitions, hackathons, workshops, seminars, etc may kindly be arranged on cyber security/ cybercrimes in various Colleges and Universities at regular intervals.

Yours faithfully,



(Deepak Virmani)
Deputy Secretary(I4C)

25/1/2021.

Copy for kind information:

1. Secretary
Department of Higher Education,
Ministry of Education,
Shastri Bhawan, New Delhi.

**LIST OF SUGGESTIVE TOPICS TO BE COVERED IN ALL THE STREAMS
(ARTS/COMMERCE/SCIENCE/ENGINEERING/MEDICAL/MANAGEMENT/BUSINES
ADMINISTRATION ETC) IN GRADUATION/POST GRADUATION**

UNIT I: Electronics Payments and safeguards therein

- i. Concept of E payments
- ii. ATM and Tele Banking
- iii. Immediate Payment Systems
- iv. Mobile Money Transfer and E-Wallets
- v. Unified Payment Interface
- vi. Cybercrimes in Electronic Payments
- vii. Precautions in Electronics Money Transfer
- viii. RBI Guidelines of Customer Protection in Unauthorized Banking Transactions
- ix. KYC: Concept, cases, and safeguards

UNIT II: Cyber Crimes and safety

- i. Introduction to cybercrimes
- i. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber terrorism, cyber obscenity, computer vandalism, Ransomware, Identity Theft
- ii. Forgery and fraud from Mobile Devices
- iii. Cyber risk associated with varied online activities and protection therefrom.
- iv. Work on different digital platforms safely
- v. Online cybercrimes against women and impersonation scams
- vi. Security awareness on Wearable gadgets
- vii. Safety in Online Financial transactions
- viii. Concept and use of Cyber Hygiene in daily life, Browser Security, Wi-Fi Security, UPI Security, Juice Jacking, Google Map Security, OTP fraud, IOT Security, E-mails.
- ix. Reporting of Cyber crime

UNIT III: Introduction to Social Networks

- i. Social Network and its contents, blogs
- ii. Safe and Proper use of Social Networks
- iii. Inappropriate Content on Social Networks
- iv. Flagging and reporting of inappropriate content
- v. Laws regarding posting of inappropriate content

UNIT IV: Introduction to Information and Technology Act, 2000(IT Act) and its use in Cyber Space

- i. Concepts as defined in IT Act
- ii. Communication Device
- iii. Computer, Cyber Security, Data Security
- iv. Secure System
- v. On line Gaming and its risks
- vi. Basic concepts of Blockchain and Cryptocurrency