F.No.D.21013/116/2021-DC

DIRECTORATE GENERAL OF HEALTH SERVICES
CENTRAL DRUGS STANDARD CONTROL ORGANIZATION

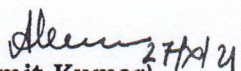New Delhi
Date: - 27.10.2021

CIRCULAR

The computer systems installed in CDSCO and Laboratories under its control are under high risk due to different types of VIRUS available over Internet, which can crash/delete all the official data in computer systems. It may also be noteworthy that that downloading of unnecessary files in some systems as well as using of harmful applications may cause serious damage to the data of computer systems of CDSCO and Laboratories under its control.

2.   Recently, we have come across a Ransomware (hoop virus) attack due to which sensitive data has got encrypted. After due consultation with CERT-IN under Ministry of Electronics and Information Technology for tackling such situations. CERT-IN has apprised us about common causes of data breach/ data leak and best practices for individual users to safeguard against data breaches and the same are mentioned below for information and strict compliance.

Best practices for individual users to safeguard against data breaches: -

i.   Use strong and unique passwords for all the online accounts. Use a password manager software. Use different passwords for different online accounts.

ii.   Enable two-factor authentication wherever available.

iii.   Regularly update all the software on computers, smart phones and other devices. Install a reputed anti-virus solution on systems, keep it updated and configure it to run scans periodically.

iv.   Be vary of clicking links received in unsolicited SMS messages or emails. Do not open email attachments from unknown senders. Limit sharing personal information on public online forums.

v.   While making online payments, ensure that the merchant website as well as the payment gateway websites are running on HTTPS and have a valid certificate (usually shown as a "green lock" symbol near the address bar in most browsers).

vi.   Do not share personal information, OTPs etc. over phone calls purporting to come from customer service, bank etc. Refuse to install any apps on smartphone / computer if asked to do so by an unknown person over phone call or in person.

vii.   Refer to website https://www.cyberswachhtakendra.gov.in for security best practices and free bot removal tools for computers and mobile devices.

This issue with the approval of Competent Authority.

(Amit Kumar)
Dy. Director Admn. (D)

Copy to:

1. Office of DCG(I).
2. All Officers/staff of CDSCO (HQ), Labs and field offices.
3. IT cell with the request to upload on the CDSCO website.