F.N. Z-18015/27/2024-NHM-II
Government of India
Ministry of Health and Family Welfare
(National Health Mission-II)

Kartavya Bhawan-1, 2nd Floor,
B-Wing, New Delhi
Dated the 17th September, 2026

OFFICE MEMORANDUM

Subject: General Guidelines of Cybersecurity and Cyber Fraud – Do's and Don'ts – reg.

The undersigned is directed to circulate herewith the Cybersecurity and Cyber Fraud – Do's and Don'ts, based on the cybersecurity for information, strict compliance and necessary action by all concerned.

2. The detailed Cybersecurity and Cyber Fraud Do's and Don'ts are attached herewith.

3. All Divisions are requested to circulate these guidelines among all officers/staff under their respective control and ensure that the prescribed cybersecurity practices are followed while accessing official IT systems and digital services.

This issues with the approval of Competent Authority.

Encl: As above

Digitally signed by
Anshu Kumar
Date: 17-09-2026
10:11:14

(Anshu Kumar)
Under Secretary to the Government of India
Tel.No.- 011-24013269
E-mail: healthmission@nic.in

To

1. AS(RG)/JS(MS)/JS (P)/ JS (GSC)/JS(MKA)/Adviser (Cost)
2. Executive Director, NHSRC

Copy to:

1. Sr. PPS to JS (Policy), MoHFW
2. Director/DS (NHM-I/II/III/IV)

General Cyber Security Guidelines

Cybersecurity Do's

1 Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers, and special characters. Change your passwords at least once in 45 days. Use multi-factor authentication, wherever available.

2 Maintain an offline backup of your critical data.

3 Keep your Operating System and BIOS firmware updated with the latest updates/patches.

4 Install enterprise antivirus client offered by the government on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures, and patches.

5 Use authorized and licensed software only.

6 When you leave your desk temporarily, always lock/log-off from your computer session.

7 When you leave office, ensure that your computer and printers are properly shutdown.

8 Keep your printer's software updated with the latest updates/patches.

9 Setup unique passcodes for shared printers.

10 Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centers.

11 Keep the GPS, Bluetooth, NFC, and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.

12 Download Apps from official app stores of google (for android) and apple (for iOS).

13 Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.

14 Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/ malware webpage, which could compromise your device.

15 Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in

16 Adhere to the security advisories published by NIC-CERT (https://nic-cert.nic.in/advisories.jsp) and CERT-In (https://www.cert-in.org.in).

Cybersecurity Don'ts

1 Don't use the same password in multiple services/websites/apps.

2 Don't save your passwords in the browser or in any unprotected documents.

3 Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material.

4 Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.

5 Don't install or use any pirated software.

6 Don't open any links or attachments contained in the emails sent by any unknown sender.

7 Don't disclose any sensitive details on social media or 3rd party messaging apps.

8 Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.

9 Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person.

Source: *Ministry of Electronics and Information technology Cybersecurity Guidelines*

Cyber Fraud Do's and Don'ts

Below is a list of the Do's and Don'ts of Cyber Fraud:

- Beware of Cyber Fraud.
  - Cyber Fraudsters can generate authentic-looking phishing emails, text messages, or websites that trick users to reveal sensitive information, such as login credentials, financial details or personal data.
  - It can create deceptive messages to trick users to click on malicious links/attachments leading to malware infections.
  - It can imitate human conversation with users to share sensitive information or to perform harmful actions.
  - It can help hackers create fraudulent documents, invoices, or payment requests for financial scams.
- Don't click on links/attachments from unknown sources.
- Always verify the authenticity of calls, emails or messages, especially those asking for sensitive information or financial transactions.
- Contact the organization directly through their official channels to validate such requests.
- Regularly update security software, install patches, and use genuine antivirus programs to protect against potential threats.
- Online Portal for filing complaint online at **cybercrime.gov.in**. Cyber fraud can be reported directly at helpline number **1930**.
- Never attend the calls looking similar to toll-free number of any bank or unauthorized company.
- Always visit the official website of the bank or any authorized company and verify the number from which the call/ SMS has been received.
- Never share OTP, PIN, CVV, Debit/Credit card details with anyone.
- Do not share any OTP/UPI PIN for receiving with money.
- Do not respond to any calls asking to confirm or share bank account, credit/debit card details or sensitive information.