



ALL INDIA INSTITUTE OF MEDICAL SCIENCES, BIBINAGAR,
HYDERABAD METROPOLITAN REGION (HMR) TELANGANA-508126, INDIA

अखिल भारतीय आयुर्विज्ञान संस्थान, बीबीनगर

हैदराबाद मेट्रोपोलिटन क्षेत्र (एचएमआर), तेलंगाना - 508126

संख्या/No. AIIMS/BBN/Admin/Misc. Corres/2024/305

दिनांक/Date : 27 July 2024

सेवा में/To,

All HoDs / Section I/c
AIIMS Bibinagar

**विषय/Sub: ADVISORY FOR PHISHING DOMAIN MIMICKING NATIONAL
INVESTIGATION AGENCY-REG**

It is informed that a copy of eHealth Division, Dept. of Health and Family Welfare, GoI, vide letter No. T-21016/108/2024-eHealth dated 22 Jul 2024 received from PMSSY-I, MoH&F vide trail email dated 23rd July 2024, regarding Advisory for Phishing Domain mimicking National Investigation Agency pertaining to staff of the institute is circulated herewith for information of the staff of your department.



भवदीय/Yours faithfully,

Siddharth
27/7/2024

(Dr. P.S Siddharth Rao)
Faculty In-charge Administration

Encls : (As above)

Copy to :-

1. PS to Executive Director, AIIMS Bibinagar for kind information of Executive Director please.
2. Deputy Director (Admin), AIIMS Bibinagar : for kind information please.
3. IT - For upload on website under staff circulars.

T-21016/108/2024-eHealth
Government of India
Department of Health and family Welfare
eHealth Division

Nirman Bhawan, New Delhi

Nirman Bhawan, New Delhi
Dated: 2024

OFFICE MEMORANDUM

Sub:- Advisory for Phishing Domain mimicking National Investigation Agency reg.

The undersigned is directed to inform that a phishing URL (<https://nia.gov.in.incidentreports.info>) created on June 10, 2024 is mimicking the National Investigation Agency (NIA) under Government of India. The phishing campaign is primarily aimed to harvest the NIC credentials of Government officials, to steal sensitive documents pertaining to Indian government and to get unauthorized access to government servers.

2. In this regard, Cyber Security Group, NIC has issued list of advisories for due awareness of all officials (Copy attached).
3. Further, it is being requested to circulate the referred advisories among all the Attached Offices/Autonomous Bodies/Subordinate Offices/Institution etc. under the administrative control of the respective PDs, for the purpose of due awareness and compliance, per se.
4. In addition to above, concerned PD may please intimate action taken in this regard to e-Health Section within 10 days.

This issues with the approval of competent authority.

Encl: As above.

(Reena Ashish Das)
Director (e-Health)
011-23062655

To,

1. AS/JS/DDG of all Program Divisions, MoHFW
2. All Director/JD/DS/DD, MoHFW
3. All Programme Divisions through eoffice Notice Board.

Advisory for Phishing Domain mimicking National Investigation Agency

Description:

A phishing URL (<https://nia.gov.in.incidentreports.info>) created on June 10, 2024 is mimicking National Investigation Agency (NIA) under Government of India. The phishing campaign is primarily aimed to harvest the NIC credentials of Government officials, to steal sensitive documents pertaining to Indian government and to get unauthorized access to government servers.

In view of above, NIC-Cyber Security Group advises following:

1. In case such a phishing mail is received, do not enter your NIC Login Credentials when redirected login prompt appears.
2. Delete these phishing emails from your inbox.
3. In case, you have already clicked the phishing URL
 - a. Take your device offline – Disable your internet connection.
 - b. Change your password - You need to change the passwords for any accounts that might have been hit in the cyberattack.
 - c. Change your passwords from a different device to ensure that the hacker can't access your new information.
 - d. Turn on multi-factor authentication for the account that might have been attacked.
 - e. Back up your files - To protect your data from the phishing attack, back up your files to an external hard drive or USB.
 - f. Scan your device with anti-virus software.
 - g. Update your Operating System, Web Browsers, and other Software with the latest security patches.
 - h. Report suspicious message to your email service provider or NIC designated mail address
 - i. Avoid sharing personal information.

By following above steps, you can effectively sanitize your system and mitigate the potential risks associated with clicking on a phishing URL.

Some ways to recognise a phishing email are given below:

- a. Be suspicious of emails that claim you must click, call, or open an attachment immediately or urgently.
- b. If a mail received from unknown source, this may be a source of phishing.
- c. If an email message has obvious spelling or grammatical errors, it might be a scam. E.g. nlc.in where the first "i" has been replaced by "l", or gov.in, where the "o" has been replaced by a "0" (zero).
- d. Images of text used in place of text (in messages or on linked web pages) may be scam.
- e. Be cautious of links shortened by using BitLy or other link shortening techniques.