



भारतीय अन्तर्देशीय जलमार्ग प्राधिकरण (पत्तन, पोत परिवहन और जलमार्ग मंत्रालय, भारत सरकार)

मुख्यालय : जलमार्ग भवन, ए-13, सैक्टर-1, नौएडा-201 301, (उ० प्र०)

INLAND WATERWAYS AUTHORITY OF INDIA

(Ministry of Ports, Shipping and Waterways, Govt. of India)

Head Office : Jalmarg Bhawan, A-13, Sector-1, Noida-201 301 (U.P.)

Website : www.iwai.gov.in | www.iwai.nic.in

Tel. : +91-120-2544036, 2543972, 2527667, 2448101 Fax : +91-120-2544009, 2544041, 2543973, 2521764

No. IWAI-11039/29/2020-Admn-Part(1)


Date: 06.05.2024

CIRCULAR

Sub: Advisory for phishing domain mimicking department of Defence-reg.

Copy of Office Memorandum no. CD-15020/17/2022-Coord dated 30.04.2024 issued by Ministry of Ports, Shipping and Waterways is **enclosed** herewith for information and further needful action.

This issues with the approval of the Competent Authority.


(Neeraj Singh)
Assistant Secretary (Admn. & Estt.)
Email id: nsingh@iwai.gov.in
Contact No: 0120-2474050

Encl: As above.

To,

All Officers/Officials of IWAI.

Copy to: - (By E-Mail)

1. Chief Engineer-Project Manager (JMVP)/ Chief Engineer (Tech.) / Hydrography Chief / Deputy Secretary (P&C) /Chief Accounts Officer / Director (NER) / Director (JMVP-II)/ Director (Technical) / Director (RE)/ Assistant Secretary (P&C) / Assistant Secretary (L&H) , IWAI, Noida.
2. Director/Dy. Director, IWAI, Kolkata / Kochi / Guwahati / Bhubaneswar, Patna.
3. Officer-In-Charge of Sub Offices, Varanasi, Prayagraj, Sahibganj, Vijayawada.
4. IT Section, IWAI, Noida
5. Hindi Cell - for Hindi translation.

Copy for kind information to: - (By E-Mail)

PPS/PS/PA to Chairman / Vice-Chairman / Member (Traffic & Logistics)/ Member (Finance) / Member (Technical) / Secretary, IWAI, Noida.

File No.:CD-15020/17/2022-Coord. (C. No. 357206)

Government of India
(भारत सरकार)
Ministry of Ports, Shipping and Waterways
पत्तन, पोत और जलमार्ग मंत्रालय

Parivahan Bhawan,
1, Sansad Marg,
New Delhi - 110001
Dated : 30th April, 2024

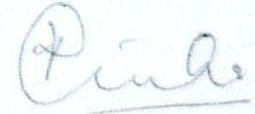
Office Memorandum

Sub: Advisory for Phishing Domain mimicking Department of Defence.

The undersigned is directed to enclose herewith a copy of advisory no. NIC-CSG/2024-04/433 dated 24.04.2024 received from NIC on the above mentioned subject and to state that a phishing URL mimicking Department of Defence under Ministry of Defence is in mass circulation since April 05, 2024. 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 an advisory for "Phishing Domain Mimicking Department of Defence".
3. In view of the above, it is kindly requested to comply and take necessary actions as advised by NIC's advisory document.
4. This issues with the approval of the Competent Authority.

Encl. : as above



(Kundan Bharti Sinha)

Under Secretary to the Government of India
kb.sinha@nic.in

To:

- i. Head of all subordinate organizations under Ministry of Ports, Shipping and Waterways.
- ii. NIC, MoPSW

Copy for information to:

- i. PPS to JS (coord. & IT), MoPSW
- ii. PPS to Director (IT), MoPSW

Advisory for Phishing Domain mimicking Department of Defence

Description:

A phishing URL mimicking Department of Defence under Ministry of Defence is in mass circulation since April 05, 2024 within various sensitive government organizations including Defence Establishment under the pretext of highlighting individuals involved in corruption cases in Defence and External affairs Ministries. 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.

Phishing URL is circulated from a compromised NIC Email ID "kmurthy.nellapu@gov.in" belonging to (Krishna Murthy Nellapu) having **Subject: "MoD Report Regarding Defence Personnel's"**.

The phishing URL consists of a "Download" button. Upon clicking Download button, a login prompt appears which asks NIC credentials of the government officials before document can be downloaded. The Phishing URL has mirrored original MoD website (www.mod.gov.in) using MoD URL.

It is pertinent to mention that closely associated phishing domains "**mod.gov.in.casereported.info, casereported.info**" similar to current phishing domain were already in adverse notice for mimicking Department of Defence.

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 Bit.Ly or other link shortening techniques.