

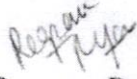
Z-11015/01/2021-Digital/IT-Part(1)
Government of India
Ministry of Agriculture & Farmers Welfare
Department of Agriculture & Farmers Welfare
Digital Agriculture Division

Krishi Bhawan, New Delhi
Dated the 26th September, 2024

CIRCULAR

This is to inform that two phishing domains are found mimicking Central Bureau of Investigation (CBI). The Phishing campaign is primarily aimed to harvest confidential documents of Indian Citizen like their Aadhar Cards, PAN cards and to gather documents of Indian Citizens like their Aadhar Cards, PAN Cards and to gather their financial to carry out malicious activities in Indian Cyber Space. The details of the phishing domains and Advisory (NIC-CSG/2024-08/502) dated 16.08.2024 regarding this have been issued by NIC and enclosed herewith for information.

Encl: As above.


(Roopam Ranjan)
Section Officer
Ph: 011-23073654
Email: so-it@gov.in

To

All the officials of DA&FW

Advisory for Phishing Domains mimicking Central Bureau of Investigation

Description:

During cyber investigation below mentioned 2 phishing domains are found mimicking Central Bureau of Investigation (CBI) under Government of India. The phishing campaign is primarily aimed to harvest confidential documents of Indian Citizens like their Aadhar Cards, PAN cards and to gather documents of Indian Citizens like their Aadhar Cards, PAN cards and to gather their financial to carry out malicious activities in Indian Cyber Space.

1. cbigovins.top/app-in2/
2. cbigovins.site/app-in2/

It is pertinent to mention that there is a "Upload Aadhar Card (JPG)" button which is collecting Front & Back Images of the Aadhar Card and the PAN Card. There is also a "Self Fund Declaration Form" which is collecting Bank Name, Account Number, Mobile Banking userid, Mobile Banking password, Internet Banking userid and password, Card Number, Expiry year/month, and the CVV number of Indian Citizens so as to carry out malicious activities in the Indian Cyber Space.

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.